Trunking, VTP, DTP and Inter-VLAN Routing

Cabrillo College

CIS 83 (CCNP 3)

Fall 2006

Rick Graziani

Cabrillo College

Note to instructors

- If you have downloaded this presentation from the Cisco Networking Academy Community FTP Center, this may not be my latest version of this PowerPoint.
- For the latest PowerPoints for all my CCNA, CCNP, and Wireless classes, please go to my web site:

  http://www.cabrillo.edu/~rgraziani/

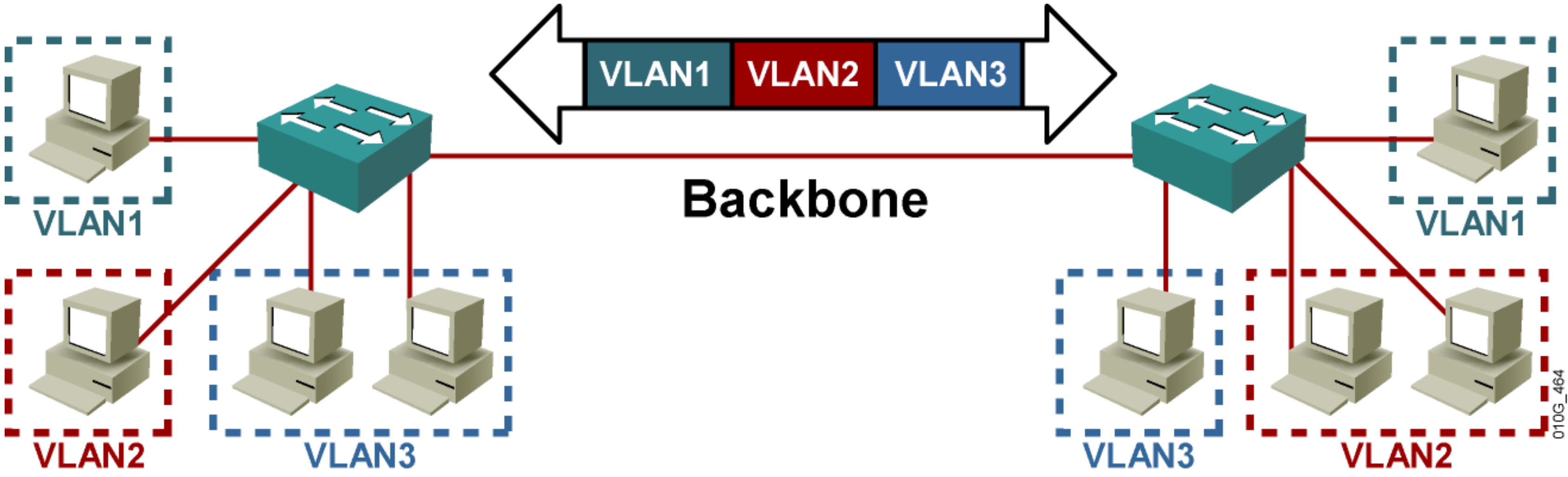
  - The username is *cisco* and the password is *perlman* for all of my materials.
- If you have any questions on any of my materials or the curriculum, please feel free to email me at graziani@cabrillo.edu (I really don't mind helping.) Also, if you run across any typos or errors in my presentations, please let me know.
- I will add "(Updated – *date*)" next to each presentation on my web site that has been updated since these have been uploaded to the FTP center.

Thanks! Rick

VLAN Trunking

Cabrillo College

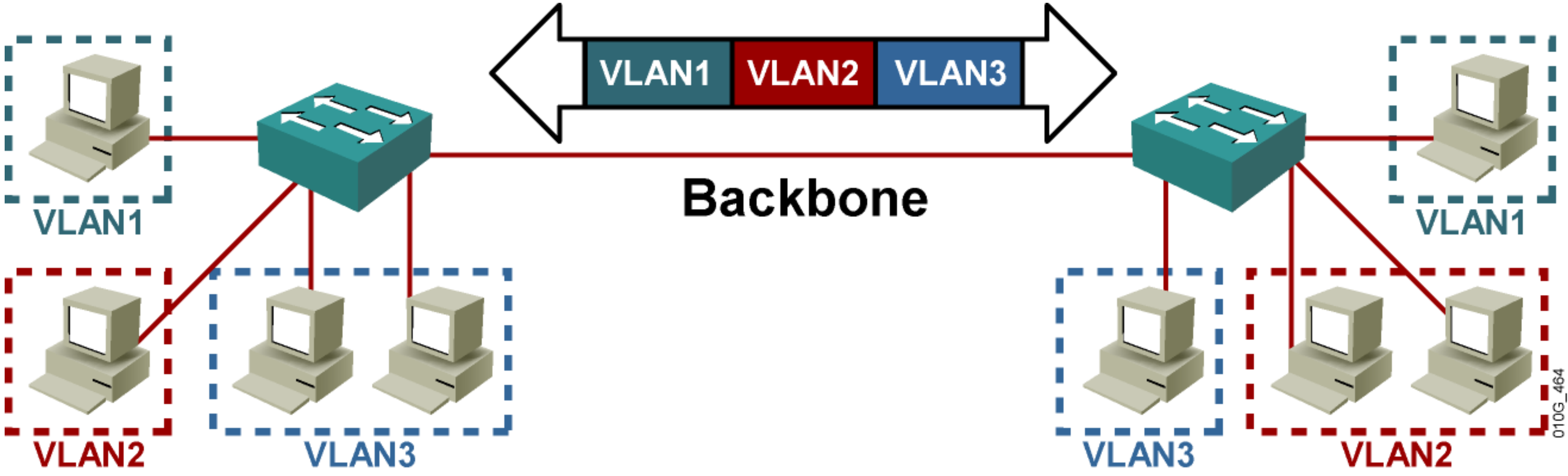
VLAN Tagging



- **VLAN Tagging** is used when a link needs to carry traffic for more than one VLAN.
- **Trunk link:** As packets are received by the switch from any attached end-station device, **a unique packet identifier** is added within each header.
- This header information designates the VLAN membership of each packet.

VLAN Tagging

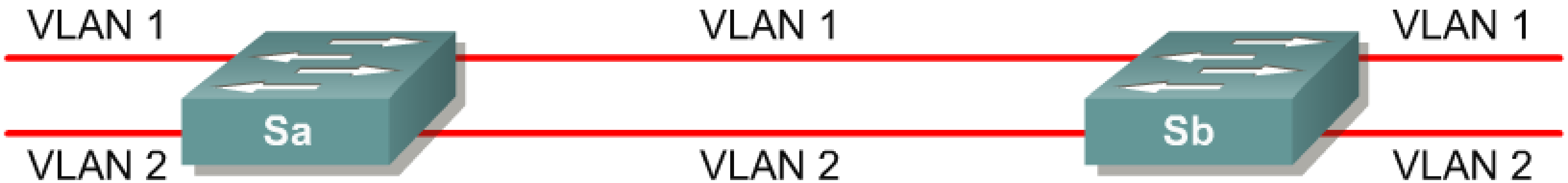
Cabrillo College



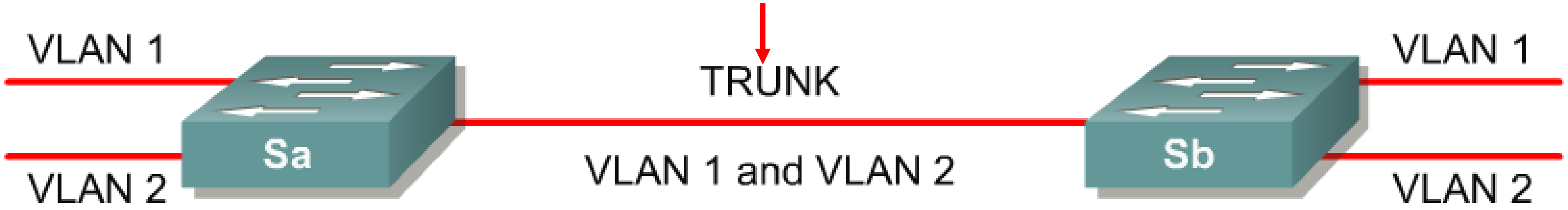
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address.
- Upon reaching the **destination node (Switch)** the **VLAN ID is removed** from the packet by the adjacent switch and forwarded to the attached device.
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications.
- This is known as a trunk link or VLAN trunking.

VLAN Tagging

No VLAN Tagging

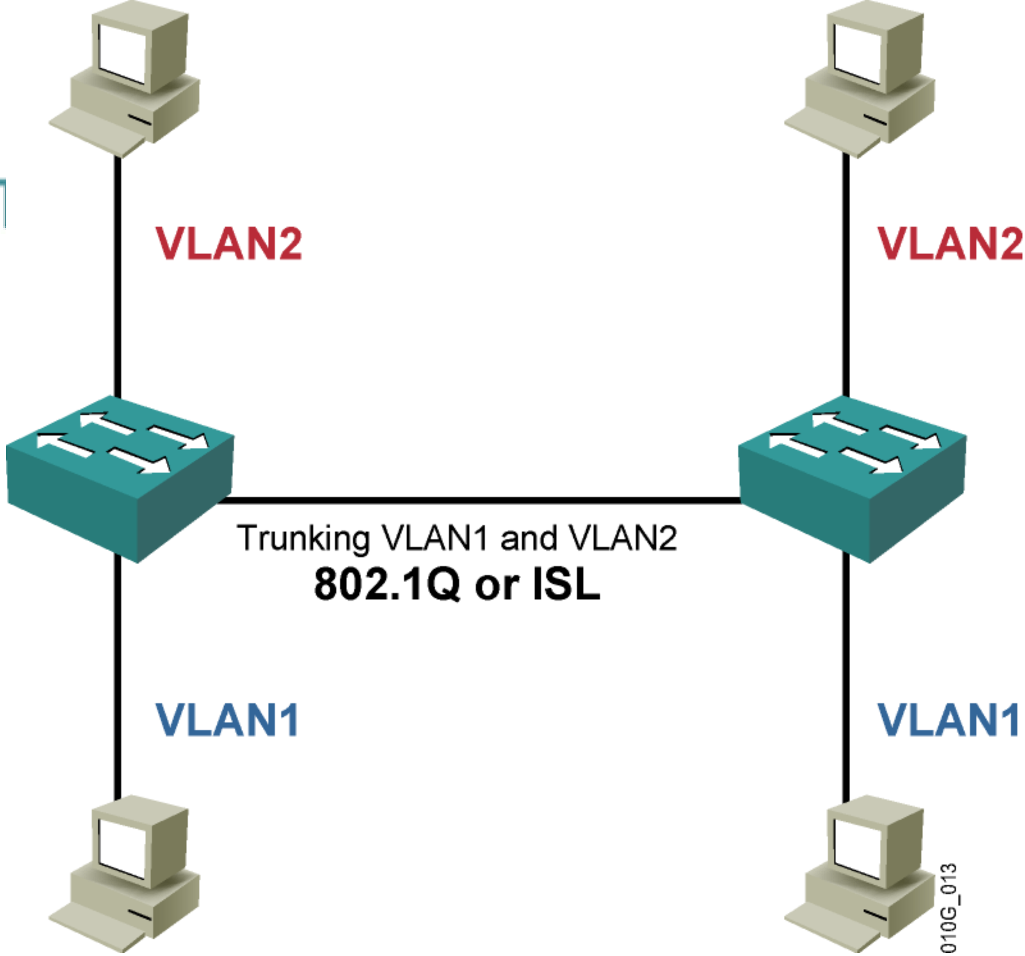


VLAN Tagging



- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN.

VLAN Tagging



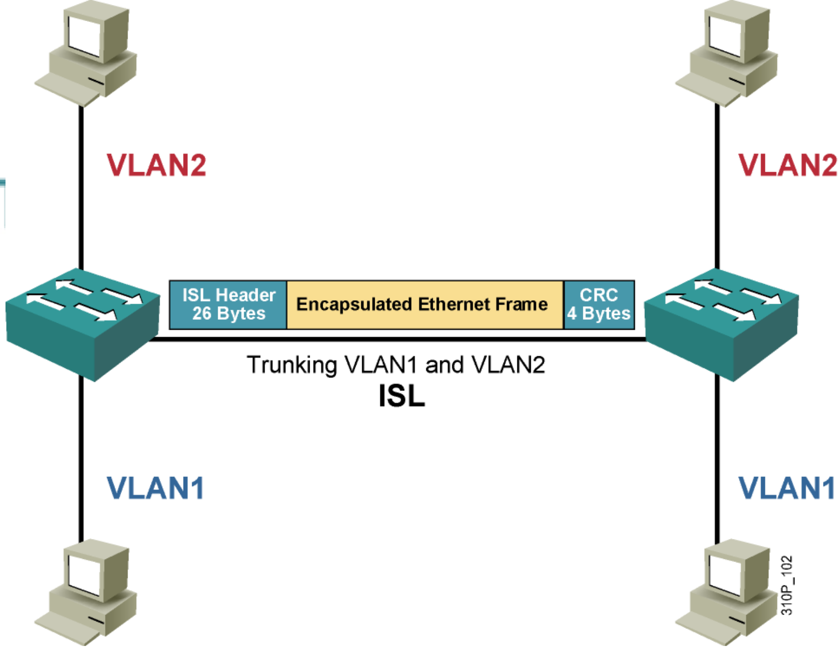
- There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and **IEEE 802.1Q**.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.
- Cisco recommends using 802.1Q.
- VLAN Tagging and Trunking will be discussed in the next chapter.

A Closer look at VLAN Tagging

ISL	802.1Q
Proprietary	Nonproprietary
Encapsulated	Tagged
Protocol independent	Protocol dependent
Encapsulates the old frame in a new frame	Adds a field to the frame header

- **There are two types of VLAN Tagging:**
  - **ISL (Inter-Switch Link) – Cisco Proprietary**
  - **IEEE 802.1Q**
- **802.1Q is recommended by Cisco and is used with multi-vendor switches.**
- **Caution**: Some older Cisco switches will only do ISL while some new Cisco switches will only do 802.1Q.

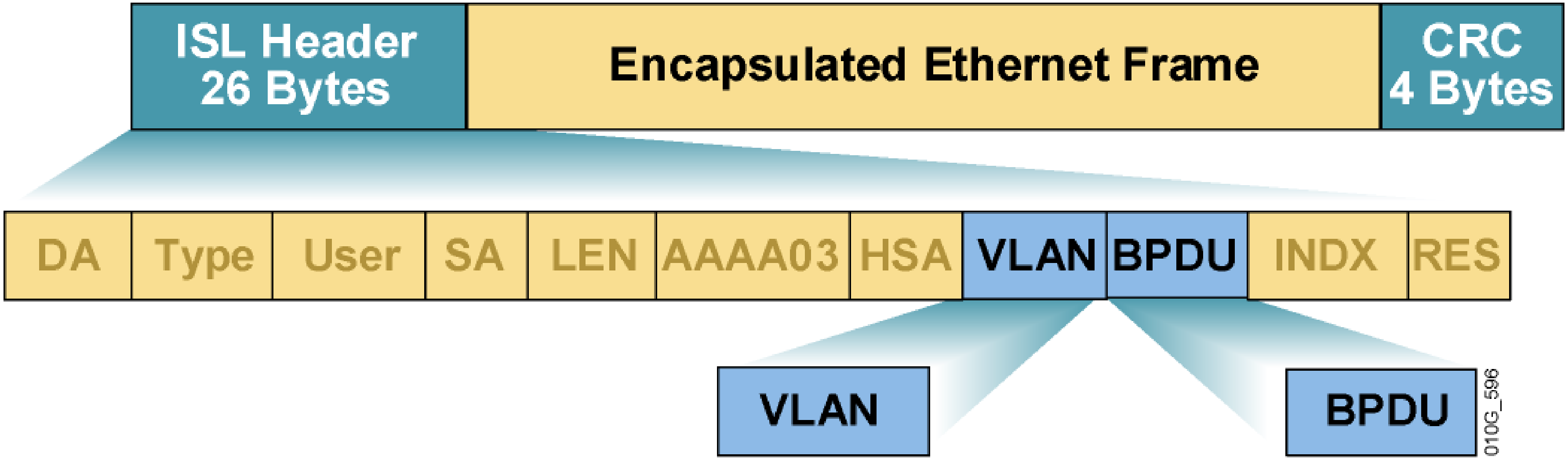
ISL (Frame Encapsulation)



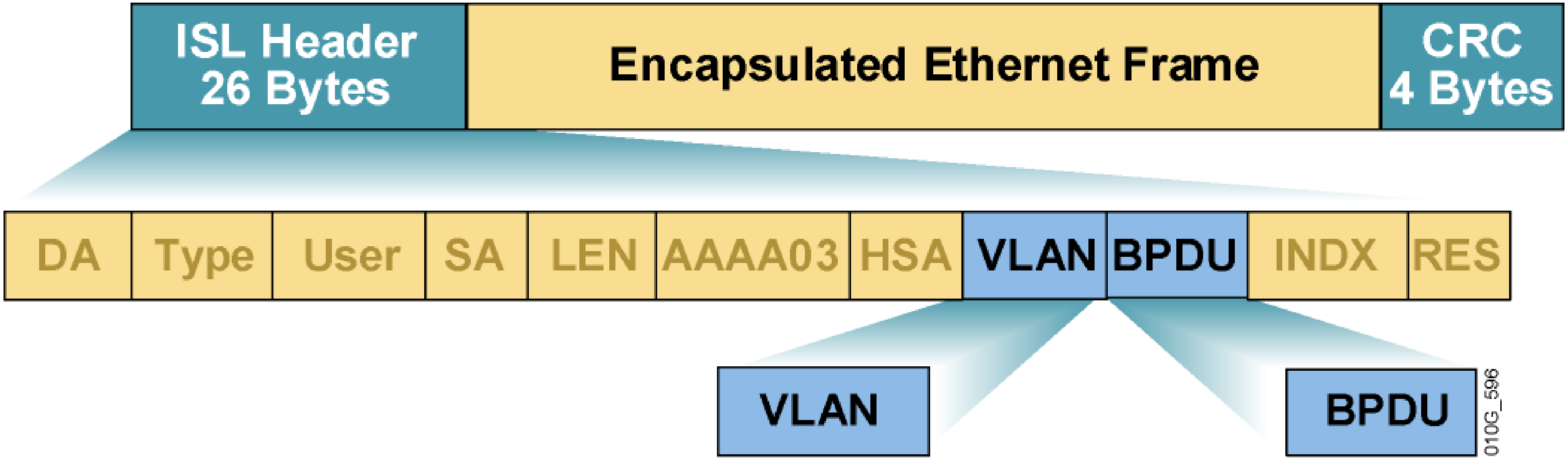
- An Ethernet frame is encapsulated with a header that transports VLAN IDs.
- The ISL encapsulation is added by the switch before sending across the trunk.
- The switch removes the ISL encapsulation before sending it out a non trunk link.
- It **adds overhead** to the frame as a **26-byte header** containing a 10-bit VLAN ID.
- In addition, a **4-byte cyclic redundancy check (CRC)** is appended to the end of each frame.
  - This CRC is in addition to any frame checking that the Ethernet frame requires.

FYI - ISL

- The following slides discuss ISL in more detail.
- This is only provided for your own information and will not be discussed, nor is it on any exam.



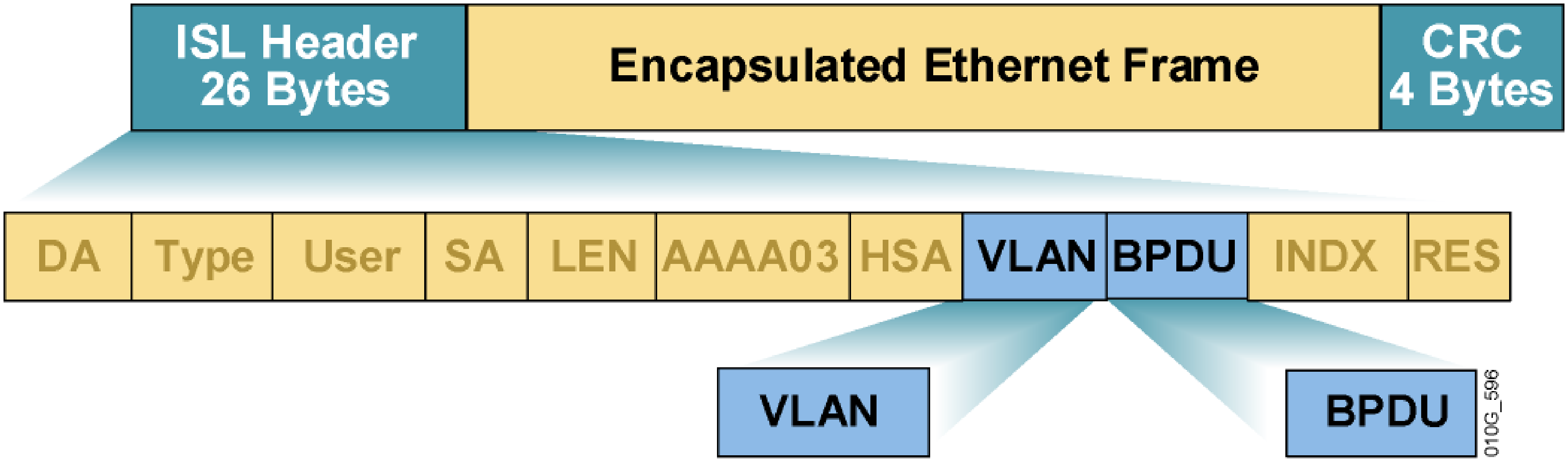
FYI - ISL



DA - Destination Address

- The DA field of the ISL packet is a 40 bit destination address.
- This address is a multicast address and is currently set to be: 0x01_00_0C_00_00.
- The first 40 bits of the DA field signal the receiver that the packet is in ISL format.

FYI - ISL

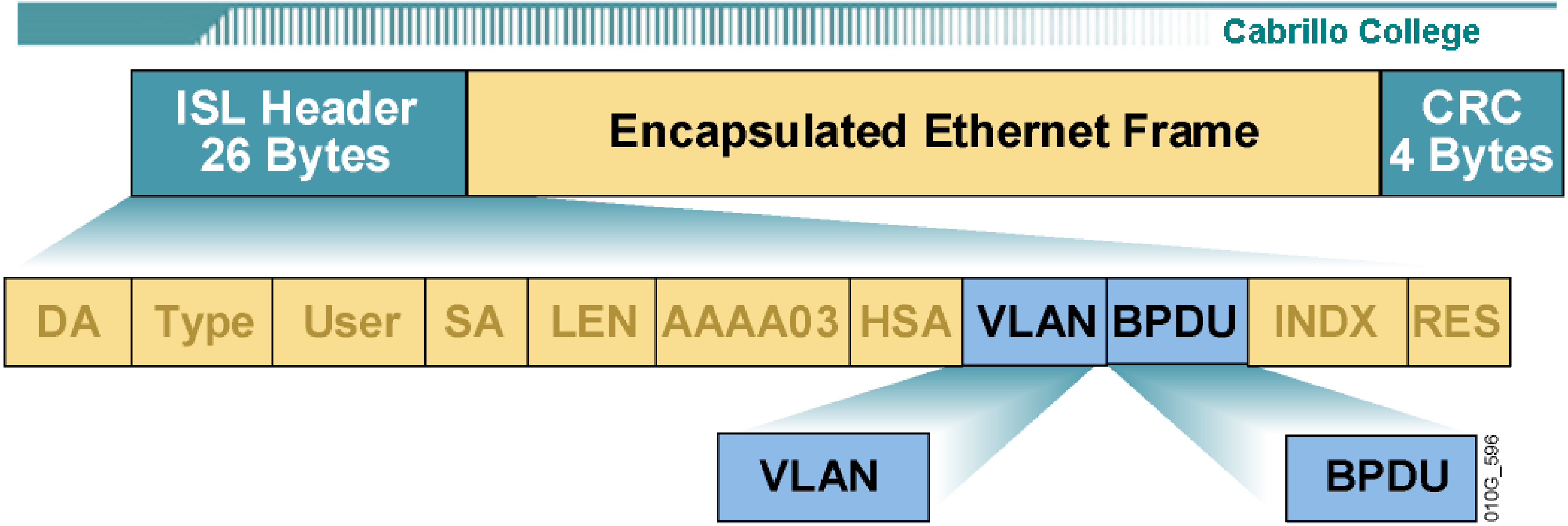


TYPE - Frame Type

- The TYPE field indicates the type of frame that is encapsulated and could be used in the future to indicate alternative encapsulations.
- The following TYPE codes have been defined:

Code Meaning
0000 Ethernet
0001 Token-Ring
0010 FDDI
0011 ATM

FYI - ISL



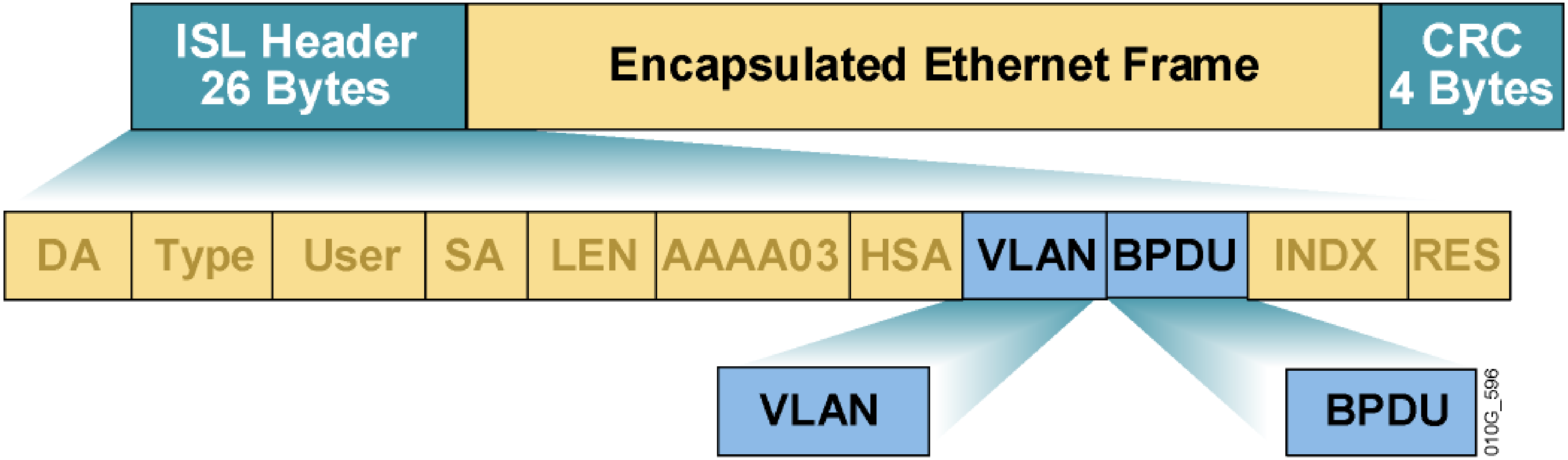
SA - Source Address

- The SA field is the source address field of the ISL packet.
- It should be set to the 802.3 MAC address of the switch port transmitting the frame. It is a 48-bit value.
- The receiving device may ignore the SA field of the frame.

VLAN - Virtual LAN ID

- The VLAN field is the virtual LAN ID of the packet.
- It is a 15-bit value that is used to distinguish frames on different VLANs.
- This field is often referred to as the "color" of the packet

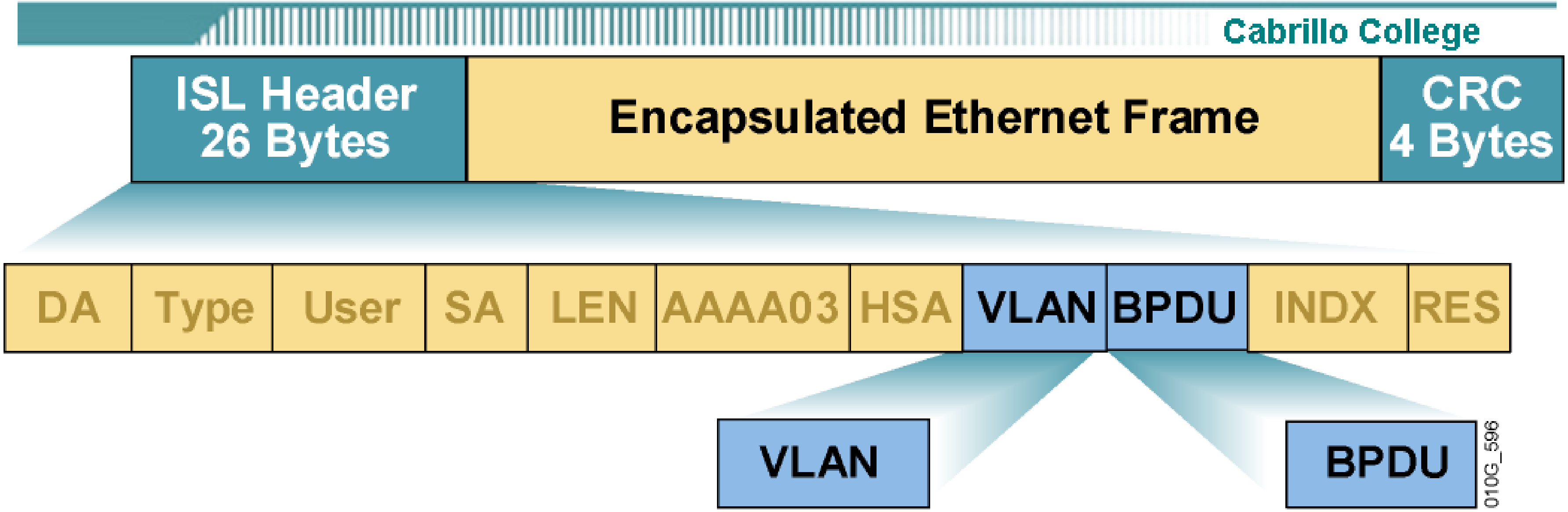
FYI - ISL



BPDU - BPDU and CDP Indicator

- The BPDU bit is set for all bridge protocol data units that are encapsulated by the ISL packet.
- The BPDUs are used by the Spanning Tree Algorithm to determine information about the topology of the network.

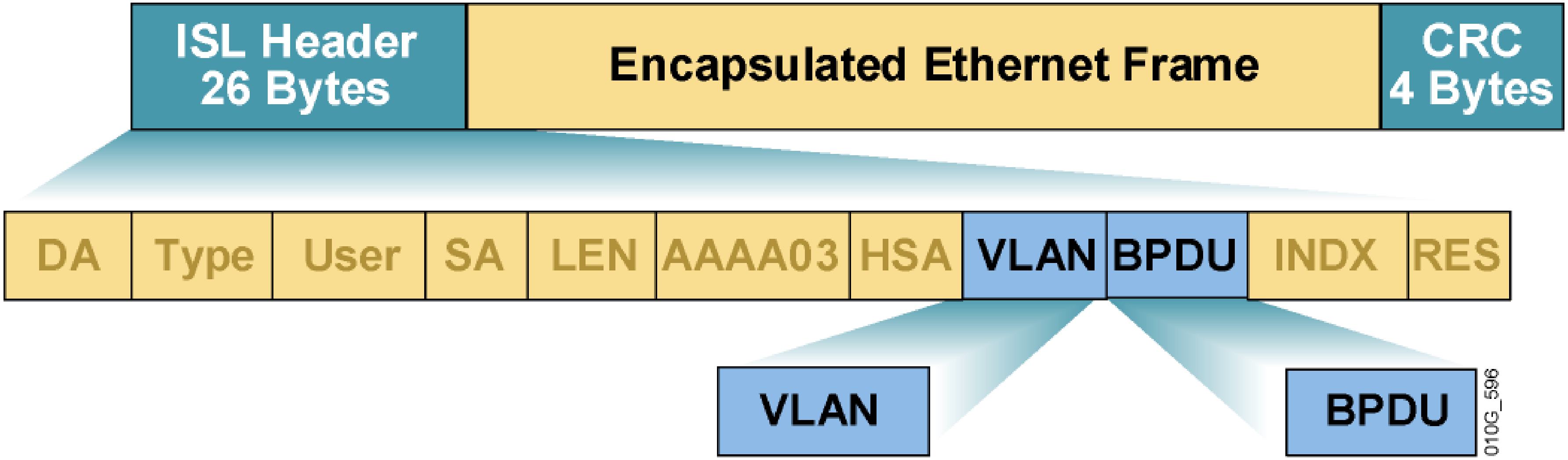
FYI - ISL



ENCAP FRAME - Encapsulated Frame

- The ENCAP FRAME is the encapsulated frame, including its own CRC value, completely unmodified.
- The internal frame must have a CRC value that is valid once the ISL encapsulation fields are removed.
- The length of this field can be from 1 to 24575 bytes long to accommodate Ethernet, Token Ring, and FDDI frames.
- A receiving switch may strip off the ISL encapsulation fields and use this ENCAP FRAME as the frame is received, associating the appropriate VLAN and other values with the received frame as indicated above for switching purposes.

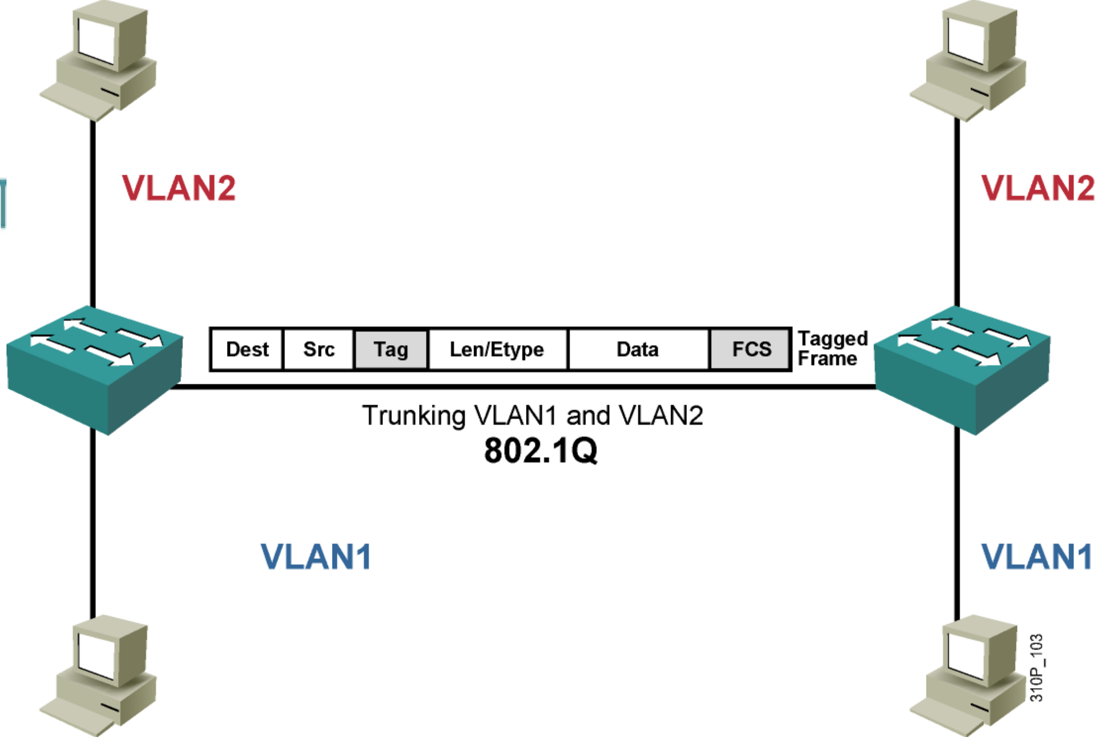
FYI - ISL



CRC - Frame Checksum

- The CRC is a standard 32-bit CRC value calculated on the entire encapsulated frame from the DA field to the ENCAP FRAME field.
- The receiving MAC will check this CRC and can discard packets that do not have a valid CRC on them.
- Note that this CRC is in addition to the one at the end of the ENCAP FRAME field.

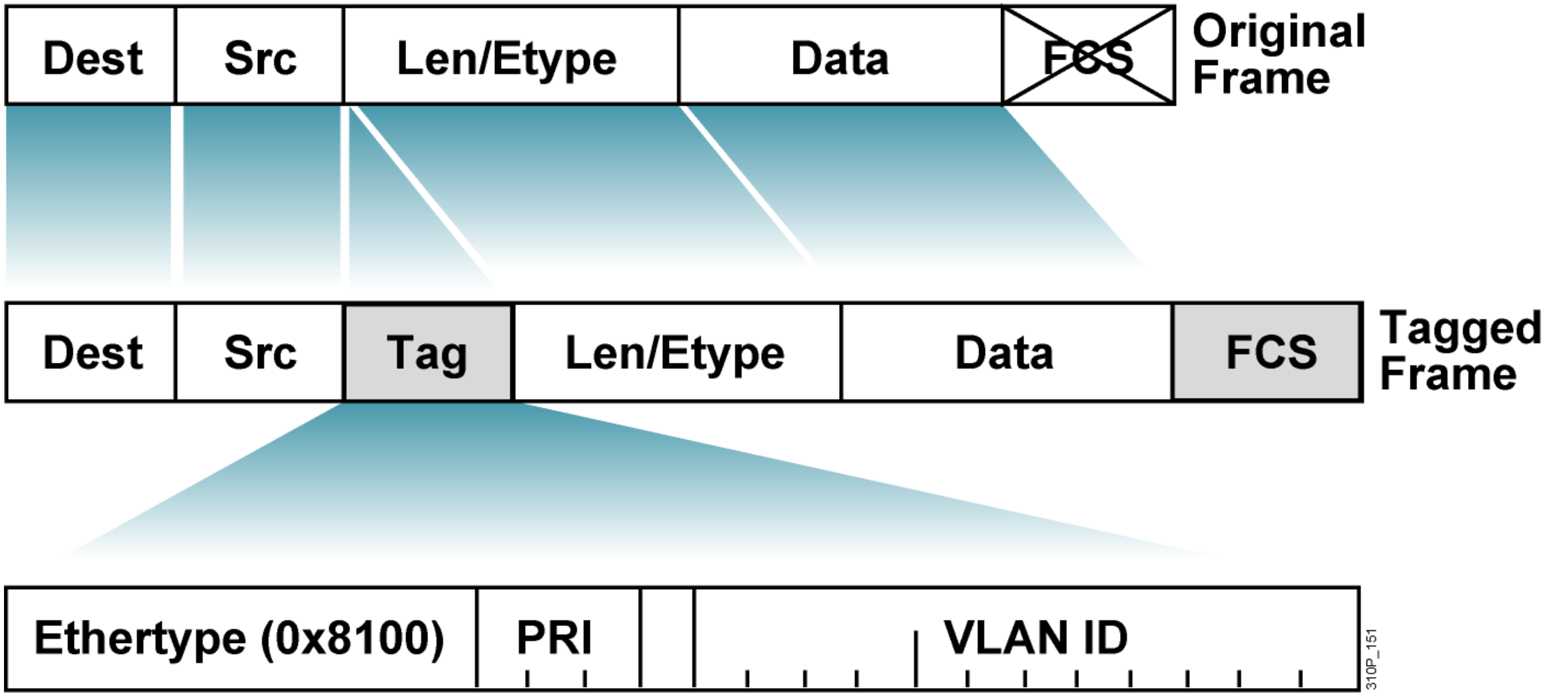
IEEE 802.1Q



- Significantly less overhead than the ISL.
- As opposed to the 30 bytes added by ISL, 802.1Q inserts only an additional 4 bytes into the Ethernet frame.
- The 802.1Q tag is inserted by the switch before sending across the trunk.
- The switch removes the 802.1Q tag before sending it out a non trunk link.

FYI – 802.1Q

- The following slides discuss 802.1Q in more detail.
- This is only provided for your own information and will not be discussed, nor is it on any exam.



FYI - 802.1Q

- A 4-byte tag header containing a tag protocol identifier (TPID) and tag control information (TCI) with the following elements:

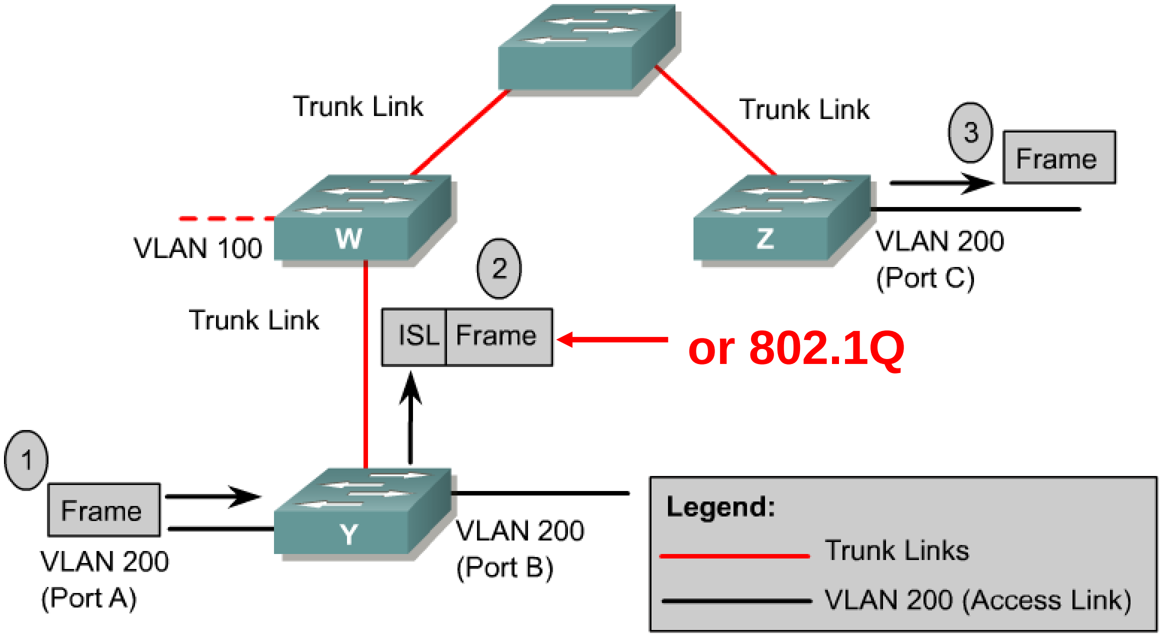
TPID

- A 2-byte TPID with a fixed value of 0x8100.
- This value indicates that the frame carries the 802.1Q/802.1p tag information.

TCI

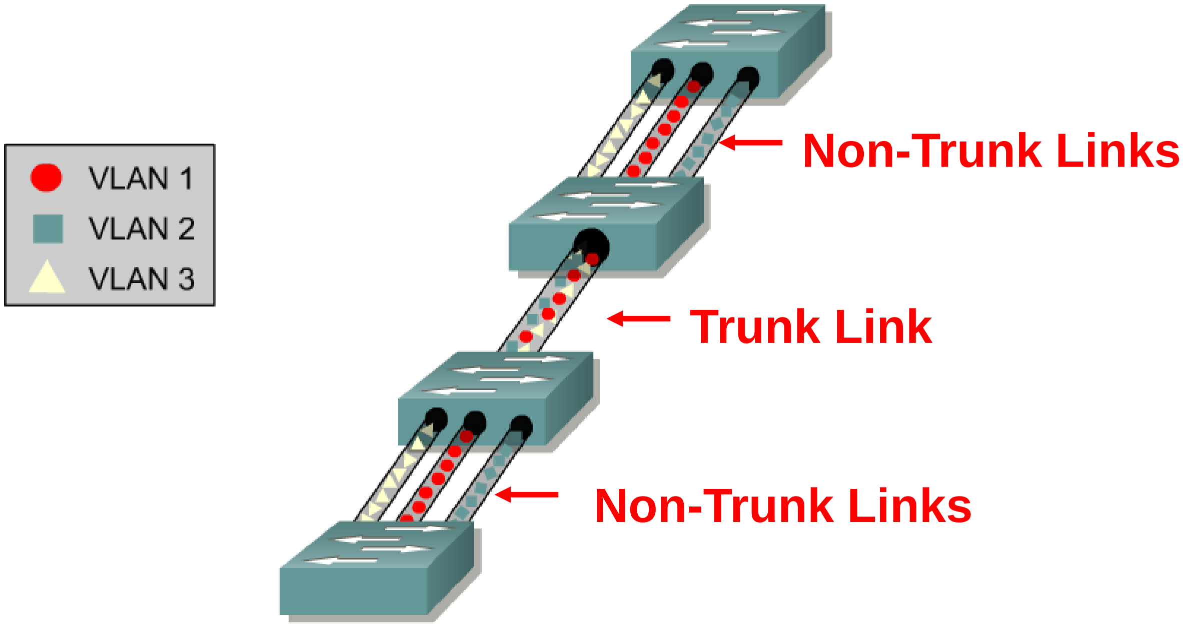
- A TCI containing the following elements:
  - Three-bit user priority (8 priority levels, 0 thru 7)
  - One-bit canonical format (CFI indicator), 0 = canonical, 1 = noncanonical, to signal bit order in the encapsulated frame (www.faqs.org/rfcs/rfc2469.html - “A Caution On the Canonical Ordering of Link-Layer Addresses”)
  - Twelve-bit VLAN identifier (VID)-Uniquely identifies the VLAN to which the frame belongs, defining 4,096 VLANs, with 0 and 4095 reserved.

Trunking operation



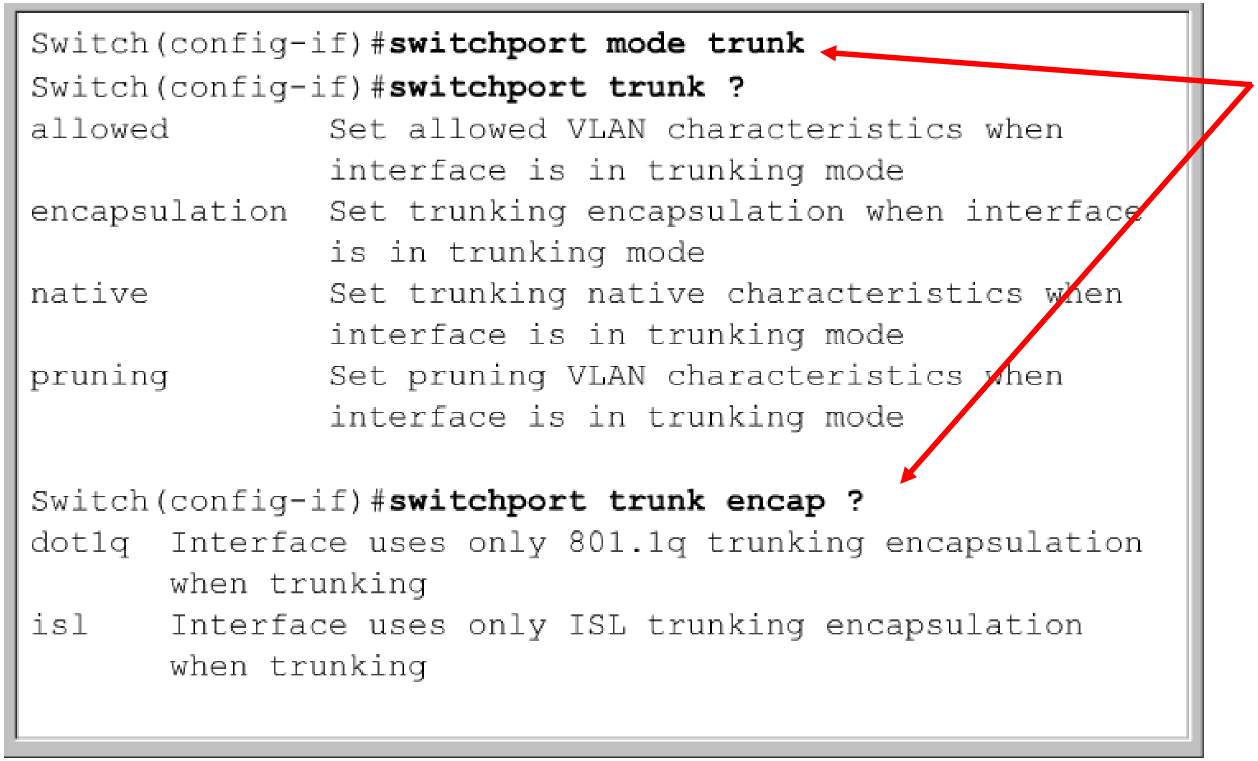
- **Trunking protocols were developed to effectively manage the transfer of frames from different VLANs on a single physical link.**
- The trunking protocols establish agreement for the distribution of frames to the associated ports at both ends of the trunk.
- Trunk links may carry traffic for all VLANs or only specific VLANs.
- VLAN tagging information is added by the switch before it is sent across the trunk and removed by the switch before it is sent down a non-trunk link.

VLANs and trunking



- It is important to understand that a trunk link does not belong to a specific VLAN.
- The responsibility of a trunk link is to act as a conduit for VLANs between switches and routers (or switches and switches).

Configuring Trunking

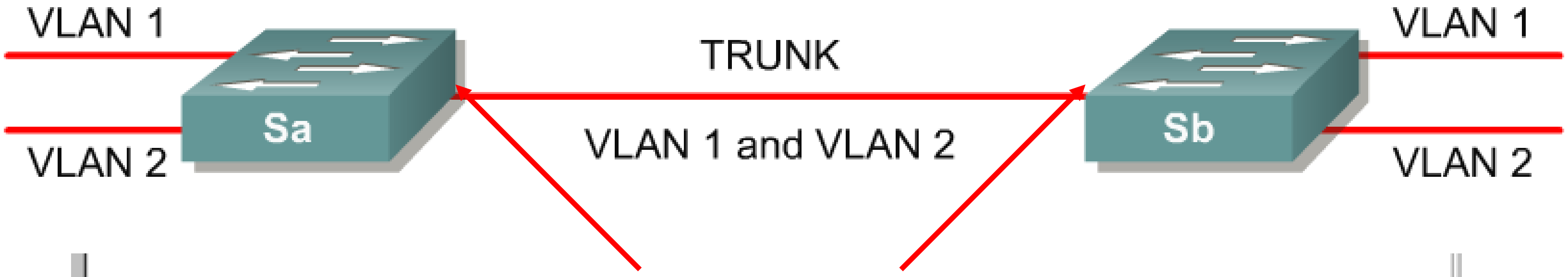


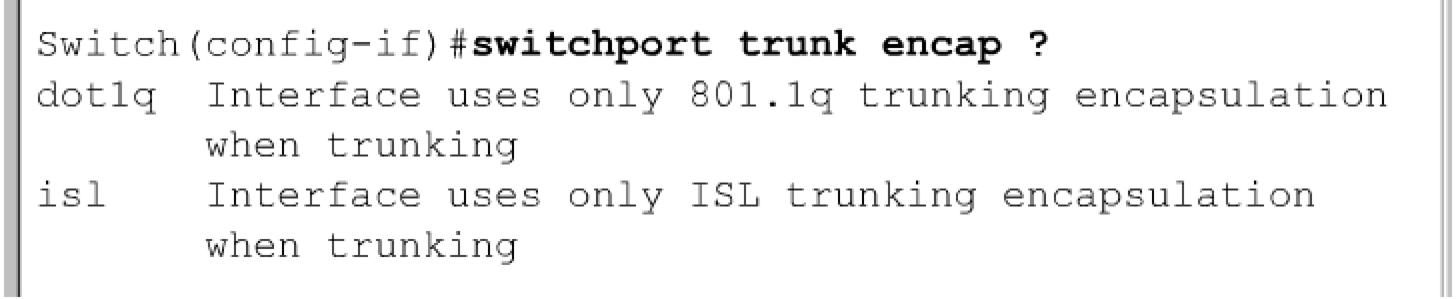
```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk ?
allowed         Set allowed VLAN characteristics when
                interface is in trunking mode
encapsulation   Set trunking encapsulation when interface
                is in trunking mode
native          Set trunking native characteristics when
                interface is in trunking mode
pruning         Set pruning VLAN characteristics when
                interface is in trunking mode

Switch(config-if)#switchport trunk encap ?
dot1q  Interface uses only 801.1q trunking encapsulation
       when trunking
isl    Interface uses only ISL trunking encapsulation
       when trunking
```

Note: On switches that support both 802.1Q and ISL, the **`switchport trunk encapsulation`** command must be done **BEFORE** the **`switchport mode trunk`** command.

- These commands will be explained in the following slides.

Configuring Trunking



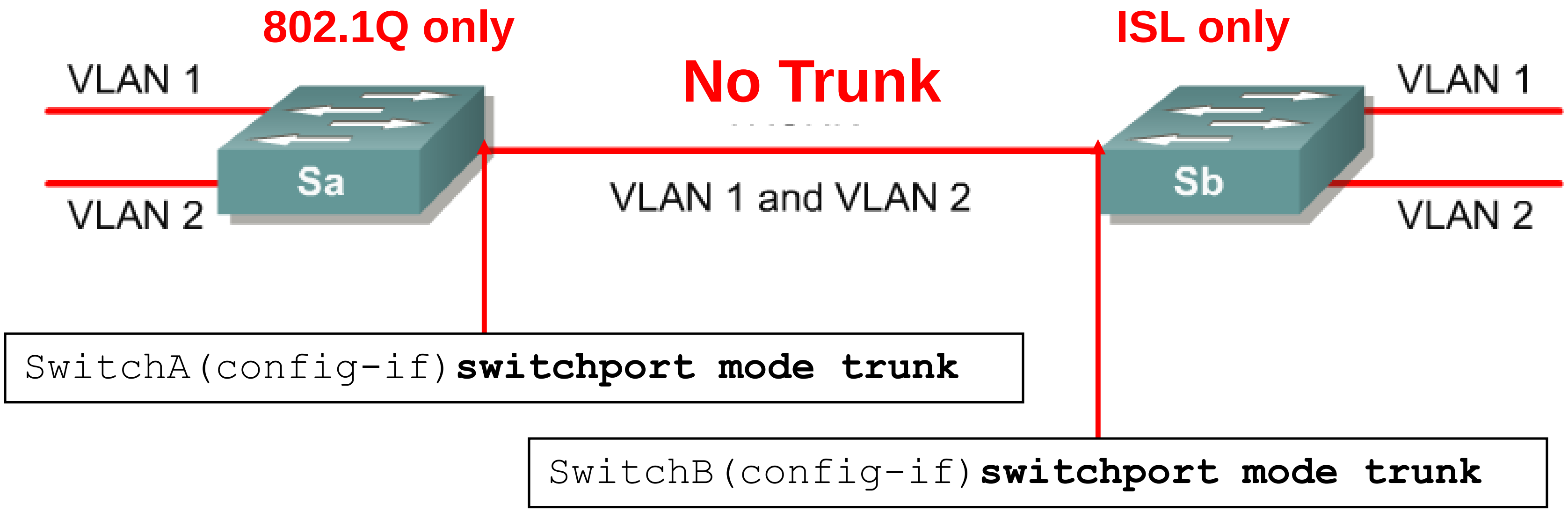


```
Switch(config-if)#switchport trunk encap ?
dot1q   Interface uses only 801.1q trunking encapsulation
        when trunking
isl     Interface uses only ISL trunking encapsulation
        when trunking
```

```
Switch(config-if)switchport trunk encapsulation [dot1q|isl]
```

- This command configures VLAN tagging on an interface if the switch supports multiple trunking protocols.
- The two options are:
  - **dot1q** – IEEE 802.1Q
  - **isl** – ISL
- The tagging must be the same on both ends.

Configuring Trunking

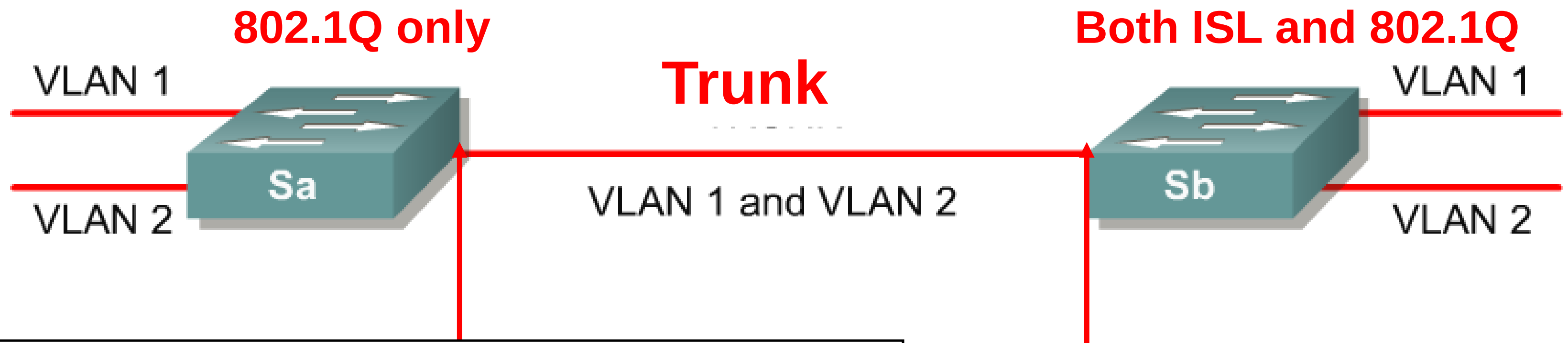


```
SwitchA(config-if)switchport mode trunk
```

```
SwitchB(config-if)switchport mode trunk
```

- If SwitchA can only be a 802.1.Q trunk and SwitchB can only be an ISL trunk, these two switches will not be able to form a trunk.

Configuring Trunking



802.1Q only

Both ISL and 802.1Q

Trunk

VLAN 1

VLAN 2

Sa

VLAN 1 and VLAN 2

Sb

VLAN 1

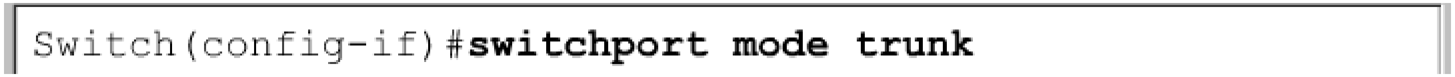
VLAN 2

```
SwitchA(config-if)switchport mode trunk
```

```
SwitchB(config-if)switchport mode trunk encapsulation dot1q

SwitchB(config-if)switchport mode trunk
```

- If SwitchA can only be a 802.1.Q trunk and SwitchB can be either ISL or 8021.Q trunk, configure SwitchB to be 802.1Q.
- On switches that support both 802.1Q and ISL, the **`switchport trunk encapsulation`** command must be done BEFORE the **`switchport mode trunk`** command.

Configuring Trunking



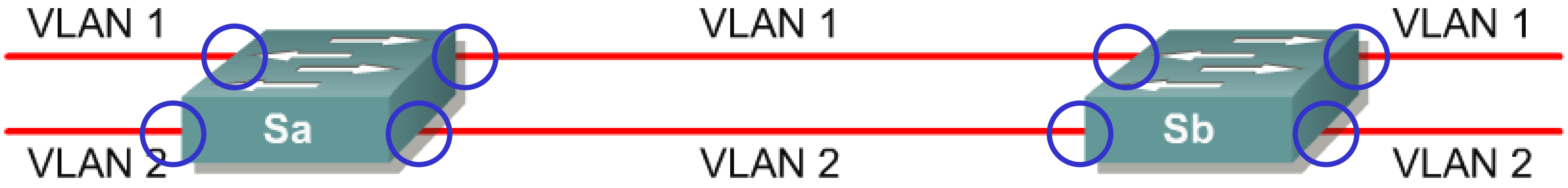
```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)switchport mode [access|trunk]
```

- By **default**, **2900XL** switchports are configured as **“access” ports**.
  - ***Not true on most other switches*** (default is dynamic desirable).
- An access port means that the port (interface) can only belong to a single VLAN.
- **Access ports** are used when:
  - Only a single device is connected to the port
  - Multiple devices (hub) are connected to the port, all belonging to the same VLAN
  - Another switch is connected to this interface, but this link is only carrying a single VLAN (non-trunk link).
- **Trunk ports** are used when:
  - Another switch is connected to this interface, and this link is carrying multiple VLANa (trunk link).

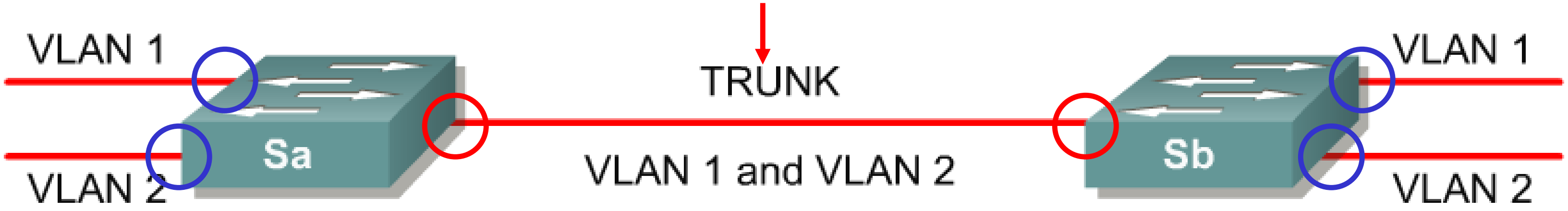
Configuring Trunking

No VLAN Tagging



```
Switch(config-if)switchport mode access ○
Switch(config-if)switchport mode trunk ○
```

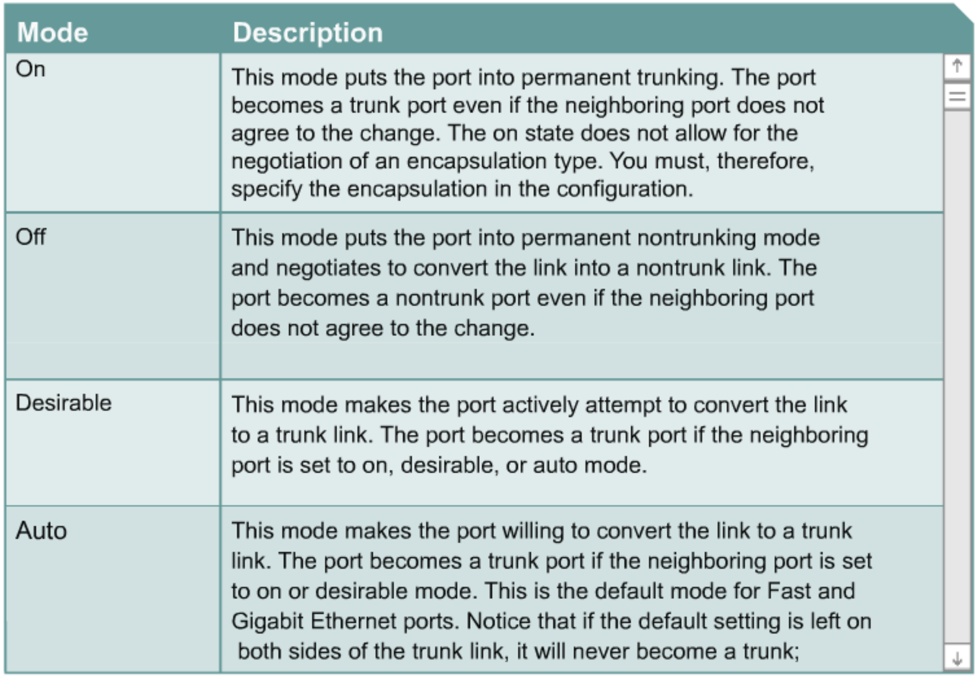
VLAN Tagging



DTP
Dynamic Trunking Protocol

To Trunk or not to Trunk (access mode), that is the question.

DTP – Dynamic Trunking Protocol



Mode	Description
On	This mode puts the port into permanent trunking. The port becomes a trunk port even if the neighboring port does not agree to the change. The on state does not allow for the negotiation of an encapsulation type. You must, therefore, specify the encapsulation in the configuration.
Off	This mode puts the port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The port becomes a nontrunk port even if the neighboring port does not agree to the change.
Desirable	This mode makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on, desirable, or auto mode.
Auto	This mode makes the port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on or desirable mode. This is the default mode for Fast and Gigabit Ethernet ports. Notice that if the default setting is left on both sides of the trunk link, it will never become a trunk;

- Note: On my web site I have created a document, DTP-CCNA.pdf that explains DTP in detail.
- The next few slides will give a brief overview of DTP.
- These slides refer to the Catalyst 2950 and 3550 switches.
- There may be some small differences with the 2900XL switches.

DTP – Dynamic Trunking Protocol

- **Ethernet trunk interfaces support several different trunking modes.**
  - **Access**
  - **Dynamic desirable (default mode on Catalyst 2950 and 3550)**
  - **Dynamic auto**
  - **Trunk**
  - **Non-negotiate**
  - **dotq-tunnel** (Not an option on the Catalyst 2950.)
- Using these different trunking modes, an interface can be set to trunking or nontrunking or even able to negotiate trunking with the neighboring interface.
- To automatically negotiate trunking, the interfaces must be in the same VTP domain. (VTP is discussed in the next section.)
- Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Cisco proprietary Point-to-Point Protocol.
- These various modes are configured using the switchport mode interface command

DTP – Dynamic Trunking Protocol

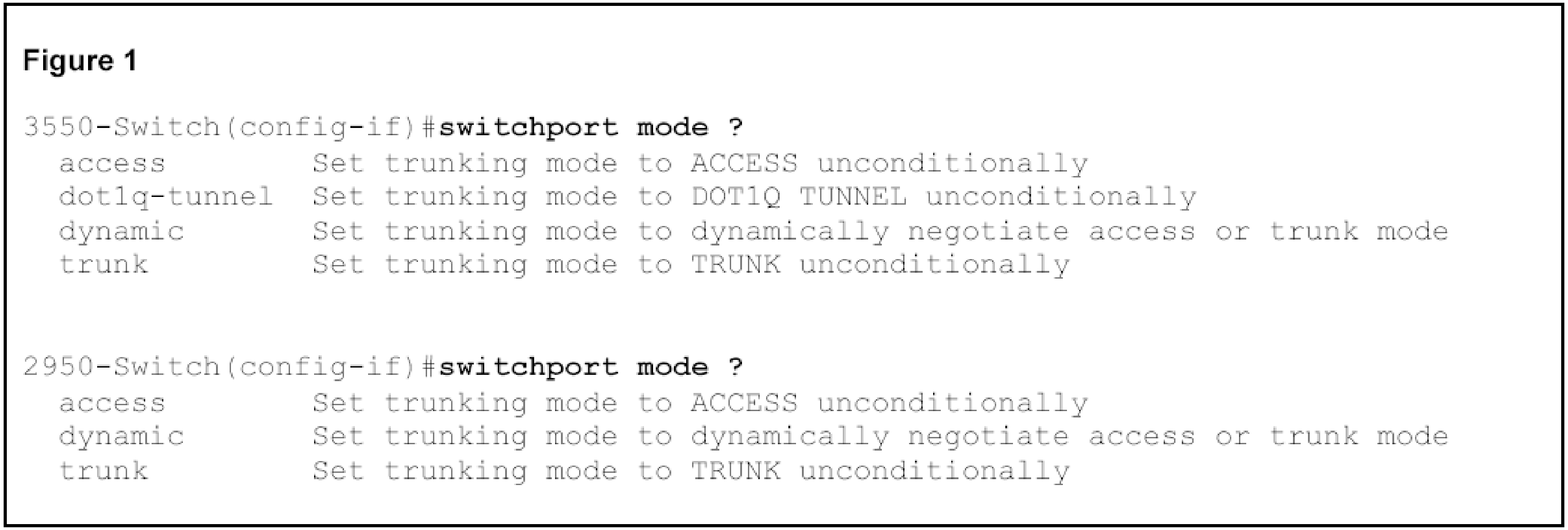


Figure 1

```
3550-Switch(config-if)#switchport mode ?
  access         Set trunking mode to ACCESS unconditionally
  dot1q-tunnel   Set trunking mode to DOT1Q TUNNEL unconditionally
  dynamic        Set trunking mode to dynamically negotiate access or trunk mode
  trunk          Set trunking mode to TRUNK unconditionally


2950-Switch(config-if)#switchport mode ?
  access         Set trunking mode to ACCESS unconditionally
  dynamic        Set trunking mode to dynamically negotiate access or trunk mode
  trunk          Set trunking mode to TRUNK unconditionally
```

- These various modes are configured using the switchport mode interface command.
- We have already discussed the two **“non-dynamic”** options:

```
Switch(config-if)switchport mode access
Switch(config-if)switchport mode trunk
```

- These options set the interface to non-trunking (access) or trunking (trunk)

DTP – Dynamic Trunking Protocol

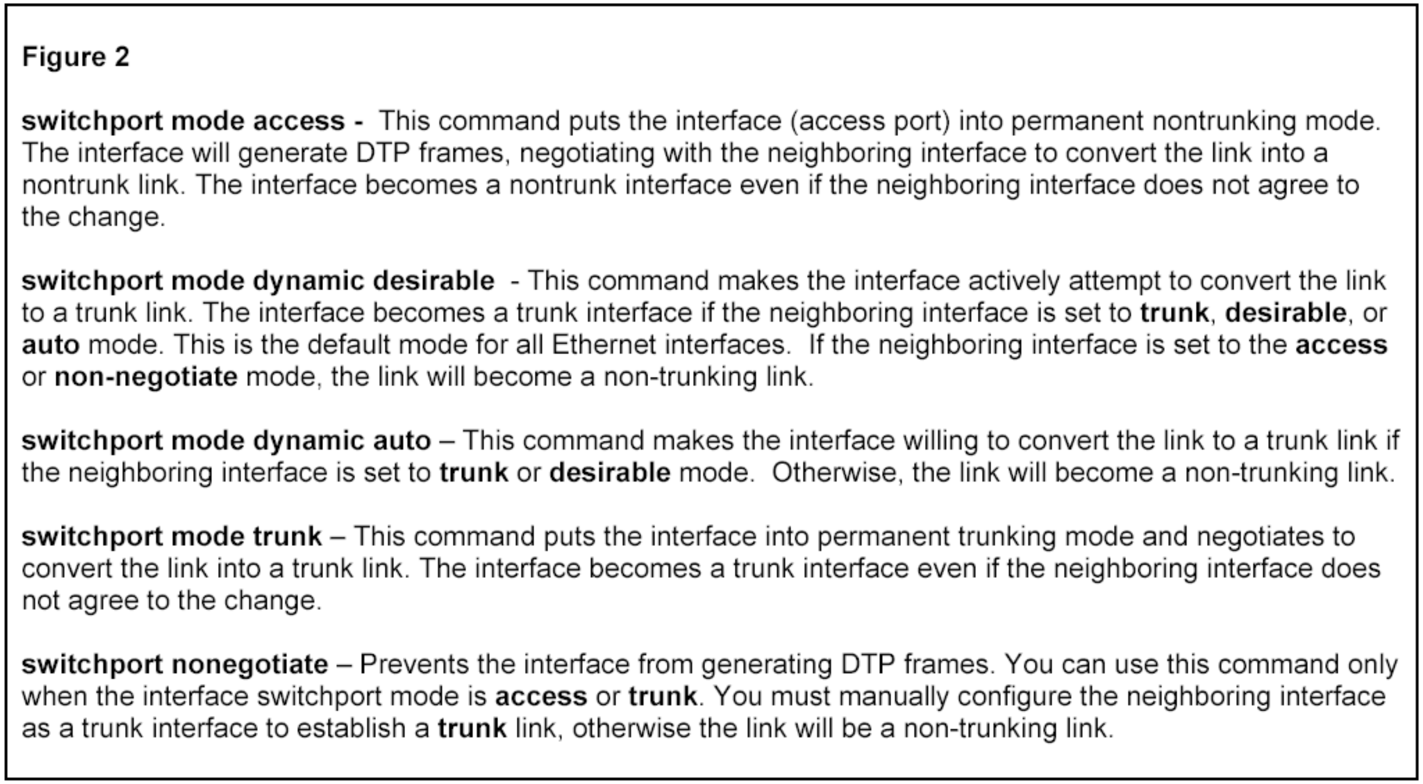


Figure 2

switchport mode access - This command puts the interface (access port) into permanent nontrunking mode. The interface will generate DTP frames, negotiating with the neighboring interface to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.

switchport mode dynamic desirable - This command makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode. This is the default mode for all Ethernet interfaces. If the neighboring interface is set to the **access** or **non-negotiate** mode, the link will become a non-trunking link.

switchport mode dynamic auto – This command makes the interface willing to convert the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode. Otherwise, the link will become a non-trunking link.

switchport mode trunk – This command puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.

switchport nonegotiate – Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a **trunk** link, otherwise the link will be a non-trunking link.

- All of these DTP modes and their various combinations can be somewhat confusing.
- Looking at some of the basic combinations can help clarify this.

DTP

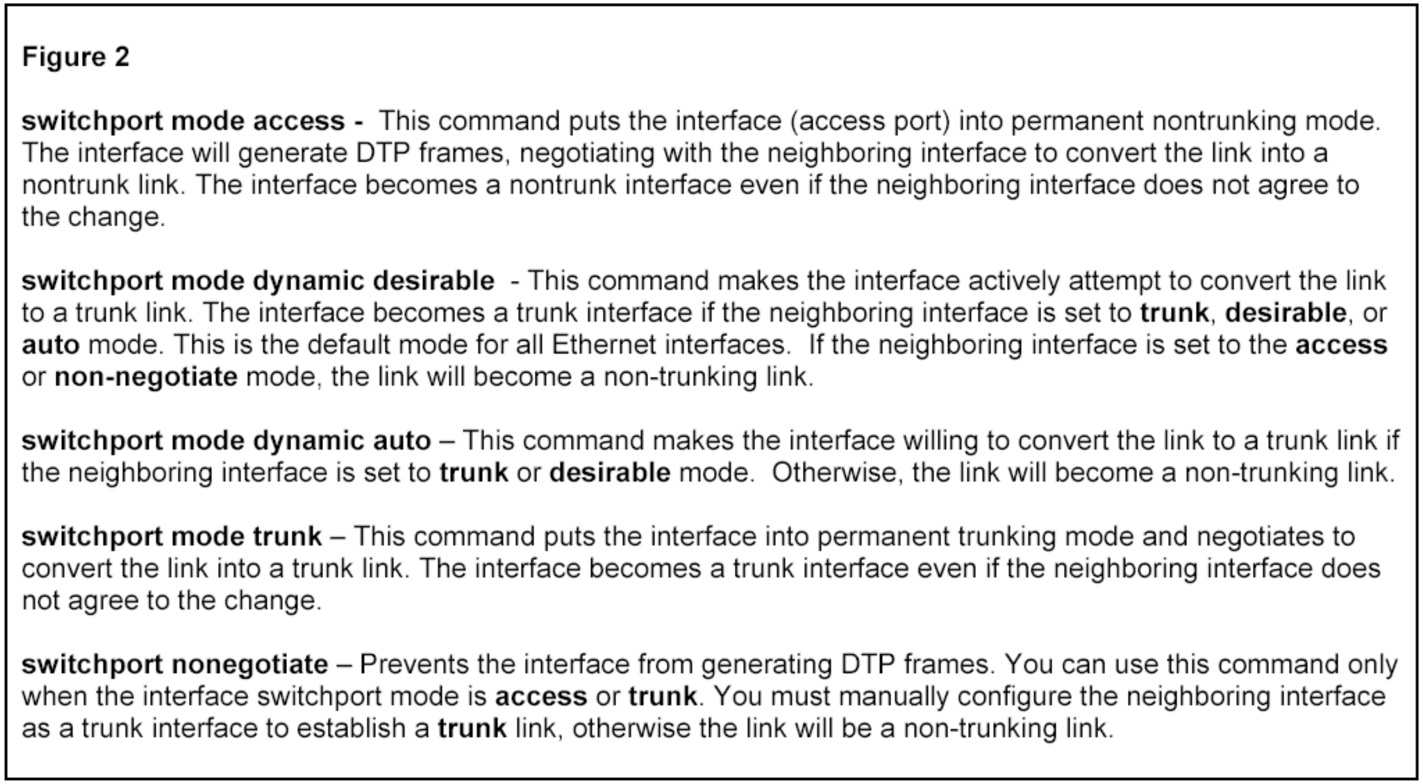


Figure 2

switchport mode access - This command puts the interface (access port) into permanent nontrunking mode. The interface will generate DTP frames, negotiating with the neighboring interface to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.

switchport mode dynamic desirable - This command makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode. This is the default mode for all Ethernet interfaces. If the neighboring interface is set to the **access** or **non-negotiate** mode, the link will become a non-trunking link.

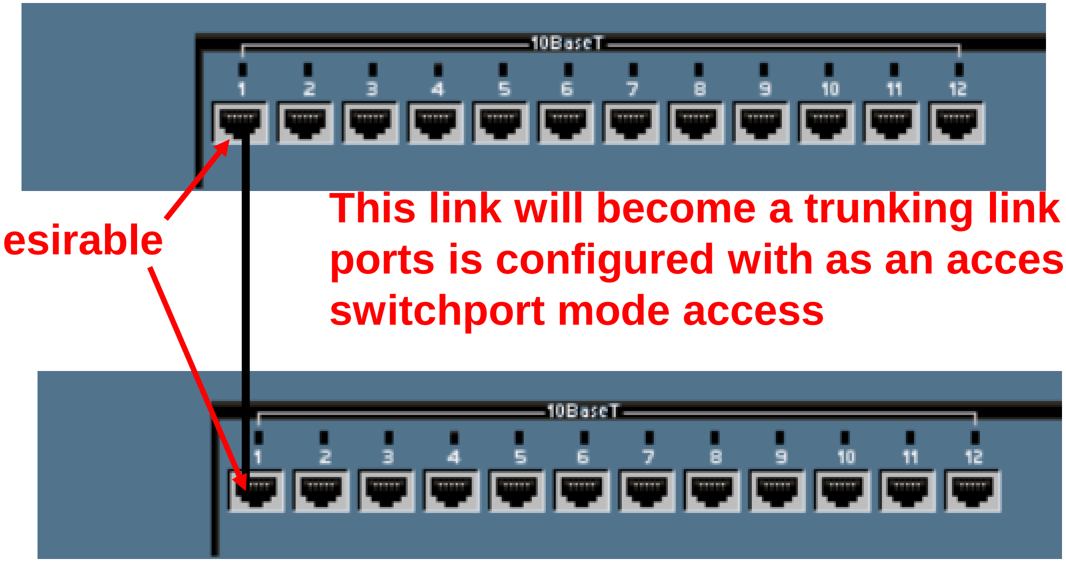
switchport mode dynamic auto – This command makes the interface willing to convert the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode. Otherwise, the link will become a non-trunking link.

switchport mode trunk – This command puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.

switchport nonegotiate – Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a **trunk** link, otherwise the link will be a non-trunking link.

- By default, Ethernet interfaces on most Cisco switches are set to **dynamic desirable** mode. (Catalyst 2950 and 3550 switches.)
- **Desirable** mode will create a trunk link if the neighboring interface is set to **desirable**, **trunk**, or **auto** mode.
- Because both interfaces by default are in **desirable** mode, this means a link between two Cisco switches will automatically become a trunk link unless configured otherwise.

Creating VLANs



Default: dynamic desirable

This link will become a trunking link unless one of the ports is configured with as an access link, I.e. switchport mode access

- By default, all ports are configured as **`switchport mode dynamic desirable`**, which means that if the port is connected to another switch with an port configured with the same default mode (or desirable or auto), this link will become a trunking link. (See my article on DTP on my web site for more information.)
- Both the **`switchport access vlan`** command and the **`switchport mode access`** command are recommended. (later)

DTP

Default for 2900XL

Default for 2950 and 3550

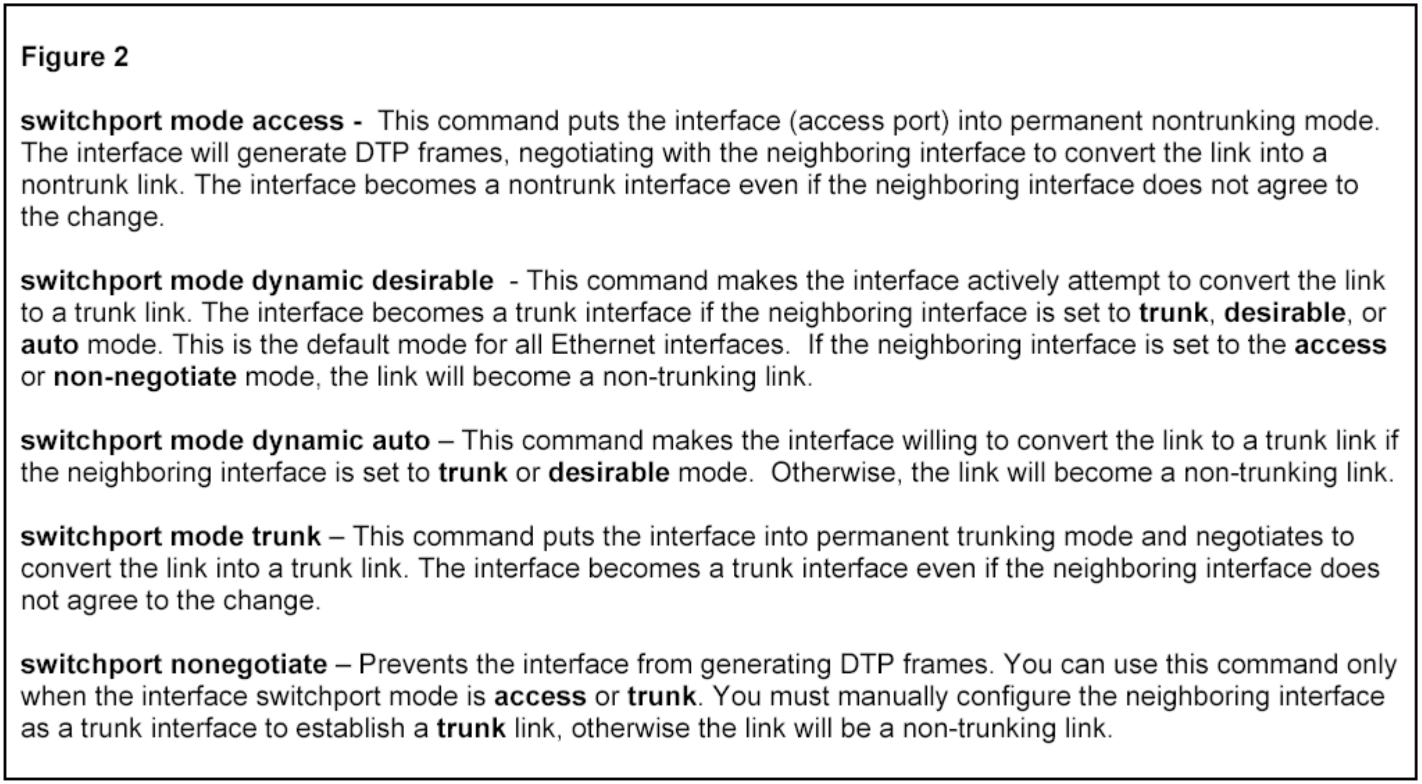


Figure 2

switchport mode access - This command puts the interface (access port) into permanent nontrunking mode. The interface will generate DTP frames, negotiating with the neighboring interface to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.

switchport mode dynamic desirable - This command makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode. This is the default mode for all Ethernet interfaces. If the neighboring interface is set to the **access** or **non-negotiate** mode, the link will become a non-trunking link.

switchport mode dynamic auto – This command makes the interface willing to convert the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode. Otherwise, the link will become a non-trunking link.

switchport mode trunk – This command puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.

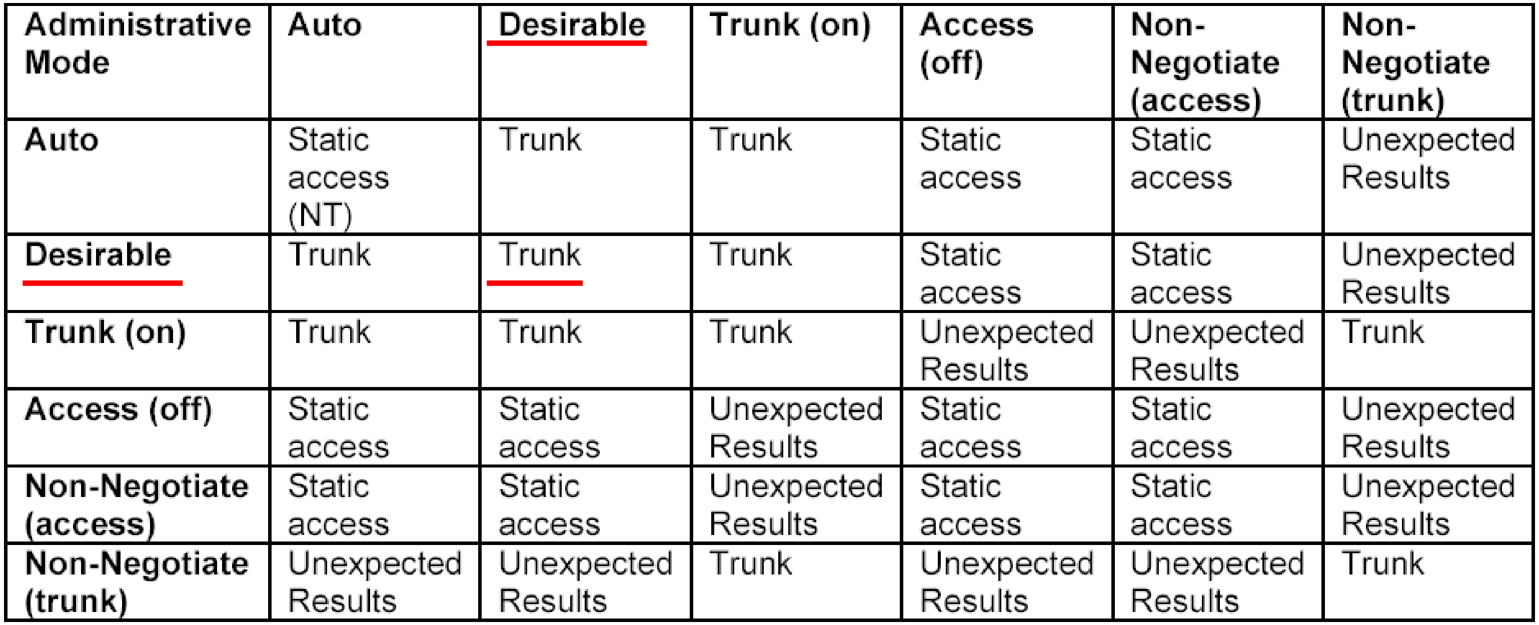
switchport nonegotiate – Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a **trunk** link, otherwise the link will be a non-trunking link.

- By default, Ethernet interfaces on Catalyst 2950 and 3550 switches default to **desirable** mode. (2900XL switches default to **access** mode.)
- **Desirable** mode will create a trunk link if the neighboring interface is set to **desirable**, **trunk**, or **auto** mode.
- On 2950 and 3550 switches, because both interfaces by default are in **desirable** mode, this means a link between two of these switches will automatically become a trunk link unless configured otherwise.

DTP

Default
2950/3550

Figure 1 Administrative Mode Combinations and their Operational Modes



Administrative Mode	Auto	Desirable	Trunk (on)	Access (off)	Non-Negotiate (access)	Non-Negotiate (trunk)
Auto	Static access (NT)	Trunk	Trunk	Static access	Static access	Unexpected Results
Desirable	Trunk	Trunk	Trunk	Static access	Static access	Unexpected Results
Trunk (on)	Trunk	Trunk	Trunk	Unexpected Results	Unexpected Results	Trunk
Access (off)	Static access	Static access	Unexpected Results	Static access	Static access	Unexpected Results
Non-Negotiate (access)	Static access	Static access	Unexpected Results	Static access	Static access	Unexpected Results
Non-Negotiate (trunk)	Unexpected Results	Unexpected Results	Trunk	Unexpected Results	Unexpected Results	Trunk

- This figure shows the various DTP trunking modes and the results of the different combinations.
- Selecting the right combination on the two ends of the link is important, as some combinations should not be used as they will have “unexpected results”.
- One combination that could result in traffic being blocked from transmitting the link is if one interface is in **access** mode and the neighboring interface is in **trunk** mode.
- For more information see my article, DTP-CCNA.pdf

DTP

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

Note: Table assumes DTP is enabled at both ends.

- **`show dtp interface` – to determine current setting**

DTP

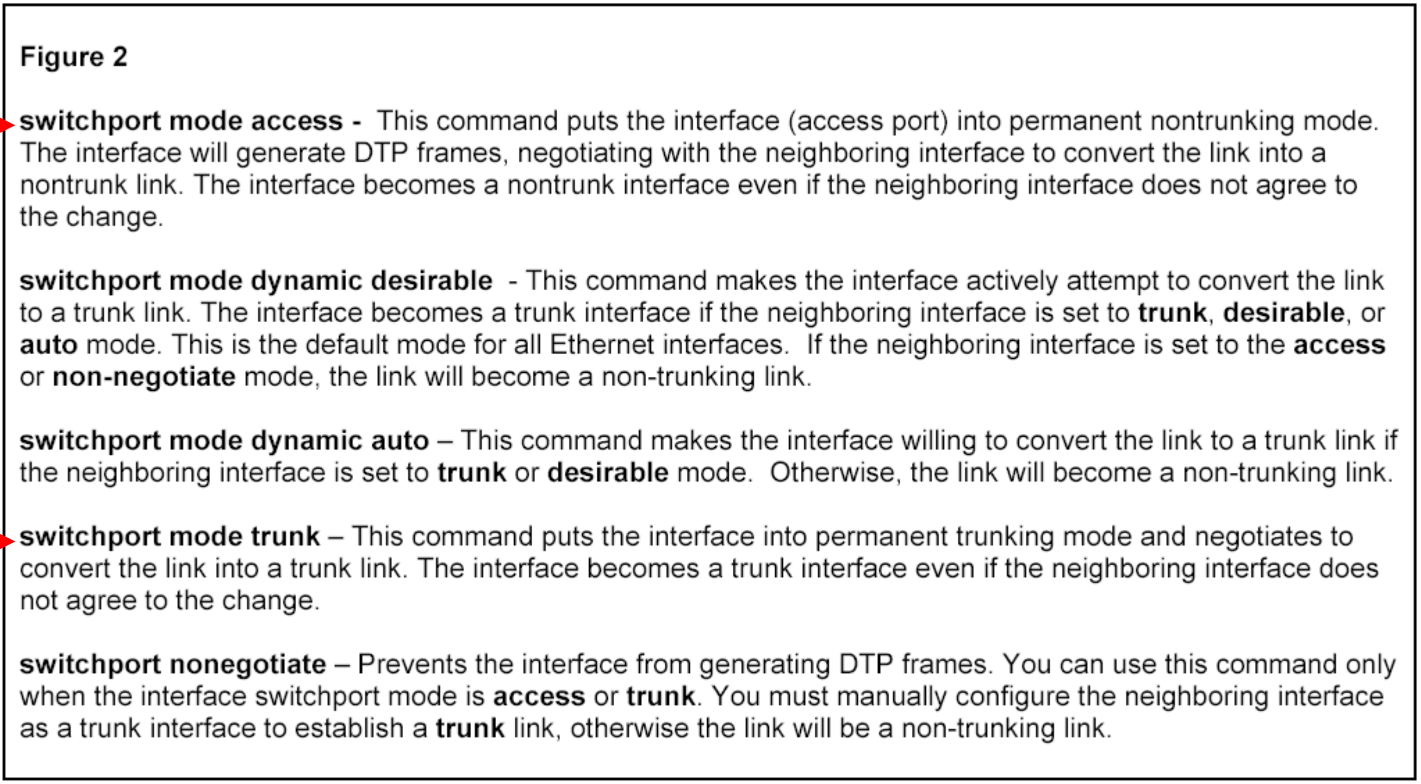


Figure 2

switchport mode access - This command puts the interface (access port) into permanent nontrunking mode. The interface will generate DTP frames, negotiating with the neighboring interface to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.

switchport mode dynamic desirable - This command makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode. This is the default mode for all Ethernet interfaces. If the neighboring interface is set to the **access** or **non-negotiate** mode, the link will become a non-trunking link.

switchport mode dynamic auto – This command makes the interface willing to convert the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode. Otherwise, the link will become a non-trunking link.

switchport mode trunk – This command puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.

switchport nonegotiate – Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a **trunk** link, otherwise the link will be a non-trunking link.

- For now, to keep it simple use either of these commands:

```
Switch(config-if)switchport mode access
OR
Switch(config-if)switchport mode trunk
```

Assigning Access Ports to VLANs

```
Switch(config)#interface range fa 0/11 - 15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10

Switch(config)#interface range fa 0/16 - 17
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

- Both of these commands “*should*” be used for access ports:
  - **`switchport mode access`**
  - **`switchport access vlan n`**

Why the `switchport mode access` command?

```
Switch(config)#interface range fa 0/11 - 15
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#end

Switch#show interface fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 10 (Accounting)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

- Without the switchport mode access command, this interface will still try to negotiate trunking.

Why the `switchport mode access` command?

```
Switch(config)#interface range fa 0/11 - 15
Switch(config-if-range)#switchport mode access

Switch#show interface fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Accounting)
```

- Now configure the range of interfaces for **permanent nontrunking, access mode**
- Notice that negotiation of trunking has been turned off and that this port will **only be a non-trunking access port**.

VTP
VLAN Trunking Protocol

Cabrillo College

Create once and send to the other switches.

Benefits of VTP (VLAN Trunking Protocol)

- ***Before discussing VTP, it is important to understand that VTP is not necessary in order to configure VLANs or Trunking on Cisco Switches.***

Benefits

- VTP is a Cisco proprietary protocol that **allows VLAN configuration** to be consistently maintained across a **common administrative domain**.
- VTP **minimizes the possible configuration inconsistencies** that arise when changes are made.
- Additionally, VTP **reduces the complexity of managing and monitoring VLAN networks**, allowing changes on one switch to be propagated to other switches via VTP.
- On most Cisco switches, VTP is running and has **certain defaults** already configured.

VTP

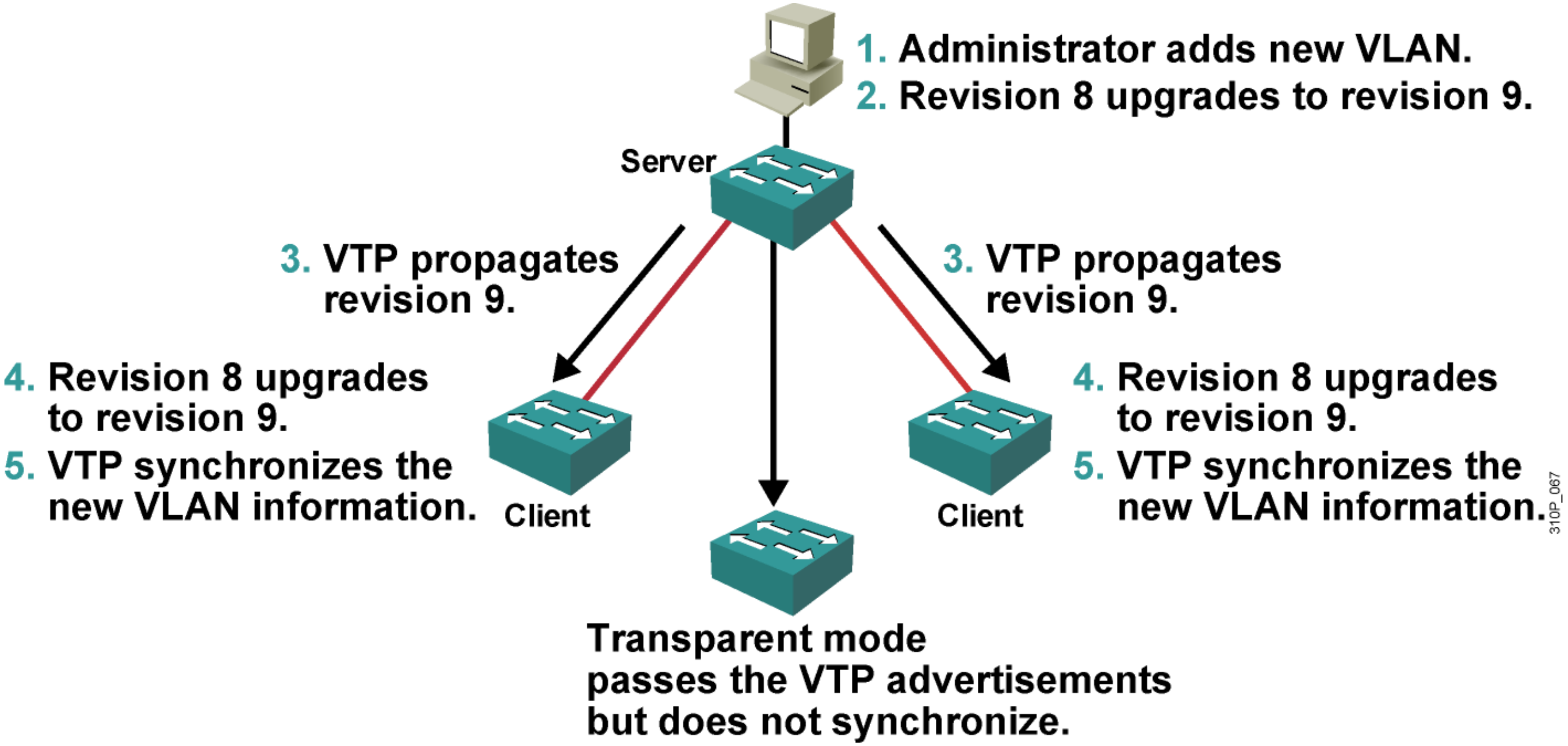
- VTP (VLAN Trunking Protocol) is used to distribute and synchronize information about VLANs that are configured throughout a switched network.
- Switches transmit VTP messages only on 802.1Q and ISL trunks.
- **Note**: VTP is not required to configure trunking between switches, but is used to simplify VLAN management.
- **VTP Server**
  - This is the default VTP mode.
  - VLANs can be created, modified, and deleted.
- **VTP Client**
  - This behaves like a VTP server without the ability to create, change, or delete VLANs.
- **VTP Transparent**
  - Switches in the VTP Transparent mode do not participate in VTP.

VTP Operation – Revision Number

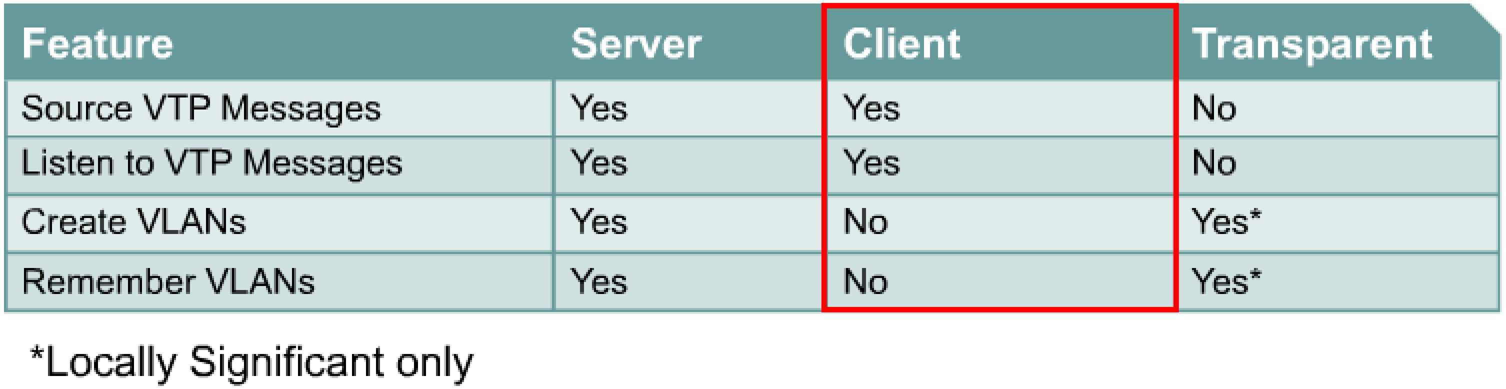
- **VTP advertisements are transmitted out all trunk connections**, including ISL, IEEE 802.1Q, IEEE 802.10, and ATM LANE trunks.
- A critical parameter governing VTP function is the **VTP configuration revision number.**
- This 32-bit number indicates the particular revision of a VTP configuration.
- A configuration revision number **starts at 0 and increments by 1 with each modification until it reaches 4294927295, at which point it recycles back to 0 and starts incrementing again.**
- **Each VTP device tracks its own VTP configuration revision number**
- **VTP packets contain the sender's VTP configuration number.**
- This information determines whether the received information is more recent than the current version.
- If the switch receives a VTP advertisement over a trunk link, it inherits the VTP domain name and configuration revision number.
- **The switch ignores advertisements that have a different VTP domain name or an earlier configuration revision number.**

VTP Operation

- VTP advertisements are sent as multicast frames.
- VTP servers and clients are synchronized to the latest revision number.
- VTP advertisements are sent every 5 minutes or when there is a change.


1. Administrator adds new VLAN.
2. Revision 8 upgrades to revision 9.
Server
3. VTP propagates revision 9.
3. VTP propagates revision 9.
4. Revision 8 upgrades to revision 9.
5. VTP synchronizes the new VLAN information.
Client
Client
4. Revision 8 upgrades to revision 9.
5. VTP synchronizes the new VLAN information.
310P_067
Transparent mode passes the VTP advertisements but does not synchronize.

VTP Operation

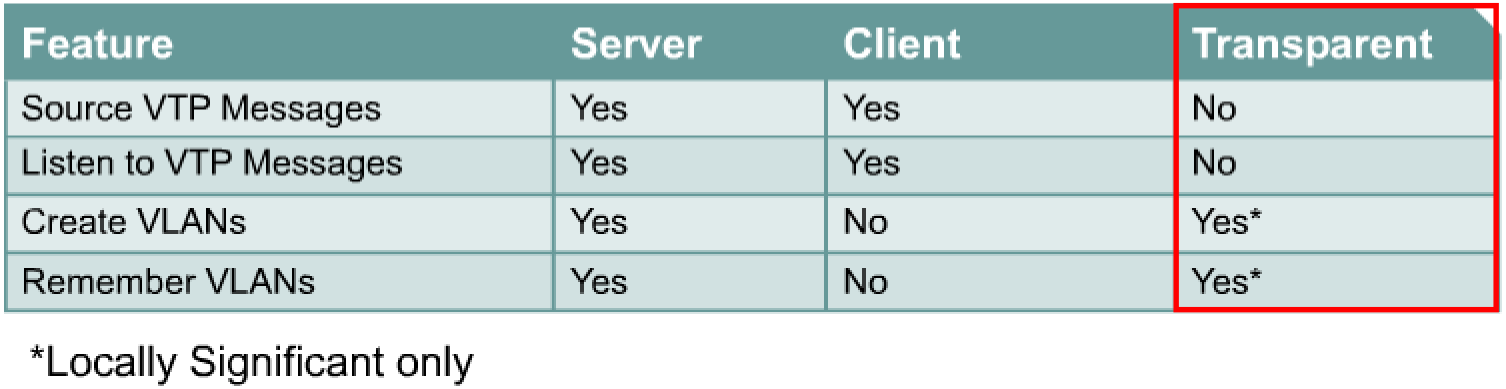


Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

- **VTP clients cannot create, modify, or delete VLAN information.**
- The only role of VTP clients is to process VLAN changes and send VTP messages out all trunk ports.
- The VTP client maintains a full list of all VLANs within the VTP domain, but it does not store the information in NVRAM.
- VTP clients behave the same way as VTP servers, but it is not possible to create, change, or delete VLANs on a VTP client.
- Any changes made must be received from a **VTP server** advertisement.

VTP Operation

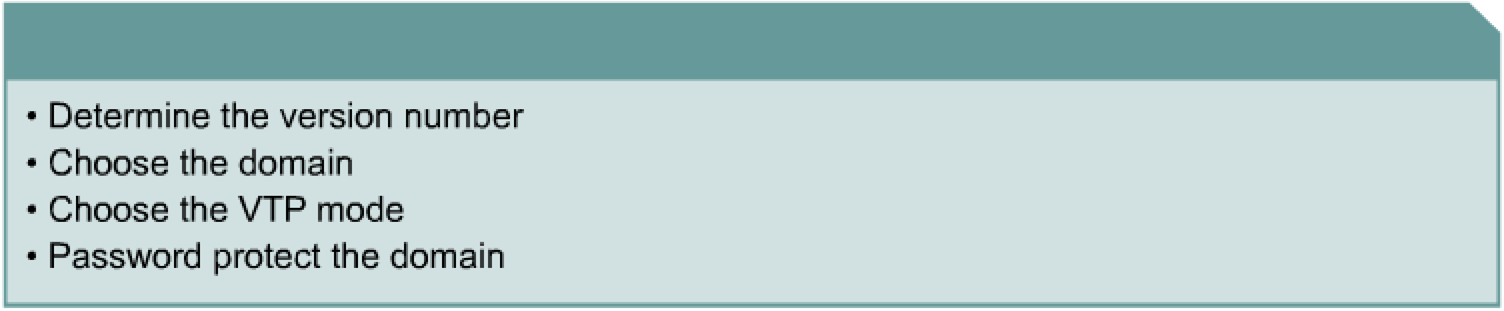


Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

- Switches in **VTP transparent mode** forward VTP advertisements but ignore information contained in the message.
- A transparent switch will not modify its database when updates are received, nor will the switch send out an update indicating a change in its own VLAN status.
- Except for forwarding VTP advertisements, VTP is disabled on a transparent switch.
- There is also an “**off**” VTP mode in which switches behave the same as in the VTP transparent mode, except VTP advertisements are not forwarded.

VTP configuration



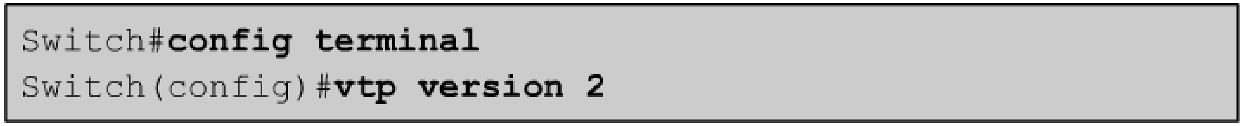
- Determine the version number
- Choose the domain
- Choose the VTP mode
- Password protect the domain

- VTP can be configured by using these configuration modes.
  - VTP Configuration in global configuration mode
  - VTP Configuration in VLAN configuration mode

- VLAN configuration mode is accessed by entering the **`vlan database`** privileged EXEC command.

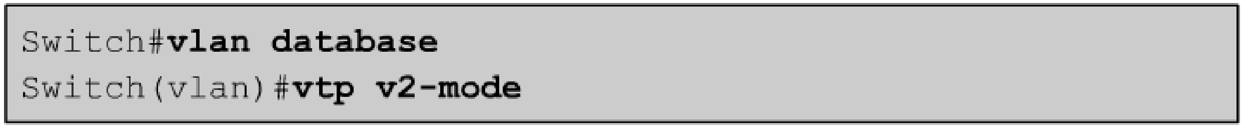
VTP configuration - Version

VTP Configuration in global configuration mode:



```
Switch#config terminal
Switch(config)#vtp version 2
```

VTP Configuration in VLAN configuration mode:

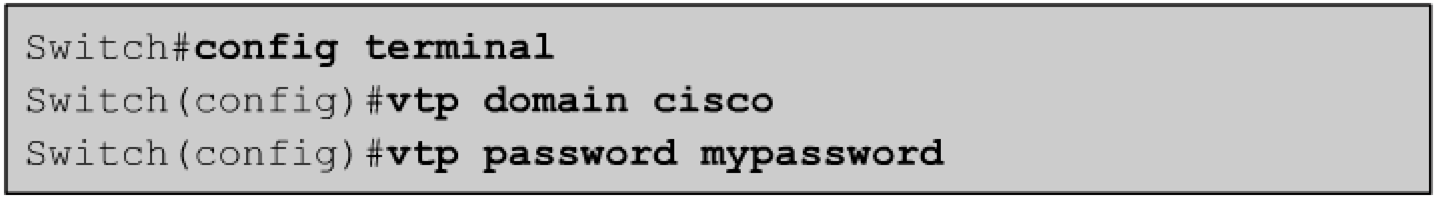


```
Switch#vlan database
Switch(vlan)#vtp v2-mode
```

- Two different versions of VTP can run in the management domain, VTP Version 1 and VTP Version 2.
- **The two versions are not interoperable in the same VTP domain**.
- The major difference between the two versions is **version 2 introduces support for Token Ring VLANs.**
- If all switches in a VTP domain can run VTP Version 2, version 2 only needs to be enabled on one VTP server switch, which propagates it to other VTP switches in the VTP domain.
- Version 2 should not be enabled unless every switch in the VTP domain supports version 2.

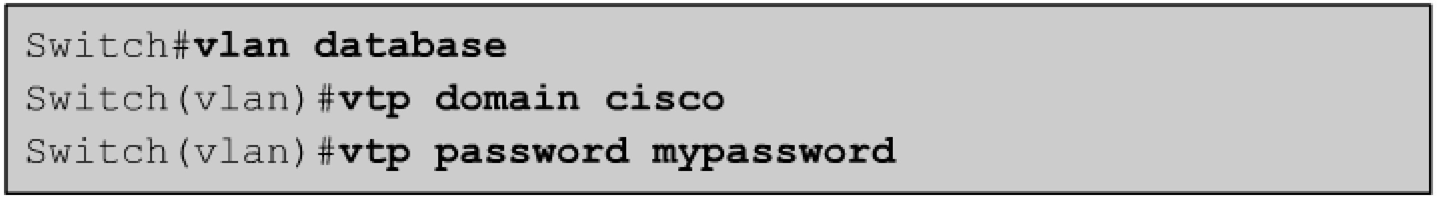
VTP configuration – Domain and Password

VTP Configuration in global configuration mode:



```
Switch#config terminal
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```

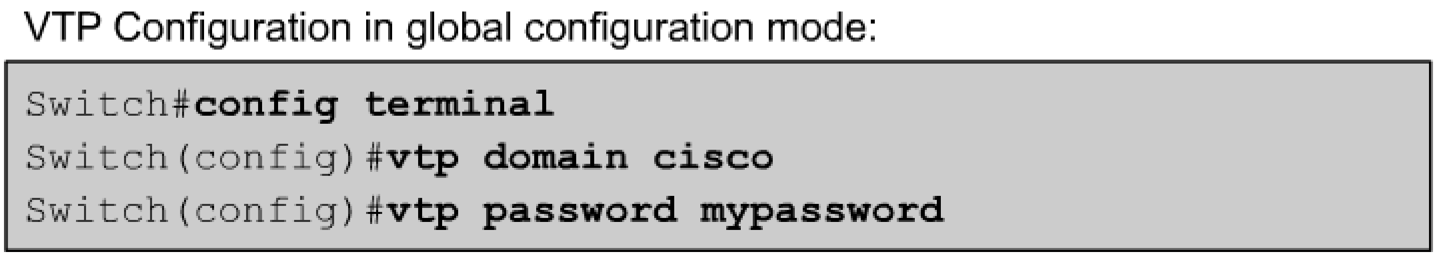
VTP Configuration in VLAN configuration mode:



```
Switch#vlan database
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

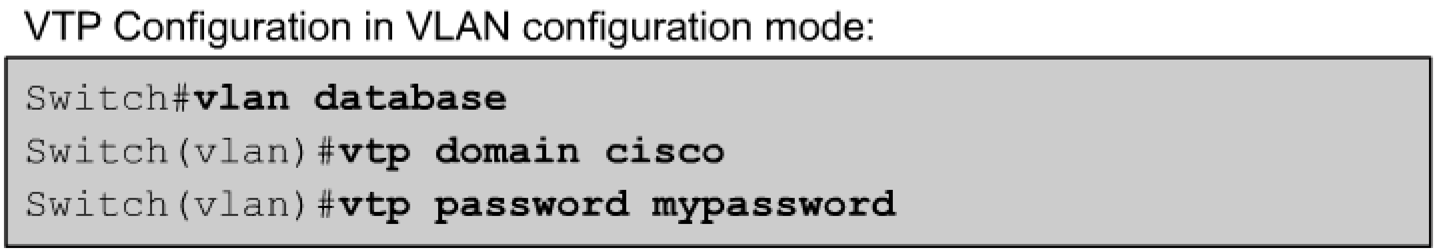
- The **domain name** can be between 1 and 32 characters.
- The **optional password** must be between 8 and 64 characters long.
- If the switch being installed is the first switch in the network, the management domain will need to be created.
- However, if the network has other switches running VTP, then the new switch will join an existing management domain.
- **Caution**: The **domain name** and **password** are case sensitive.

VTP configuration – Domain and Password



VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```



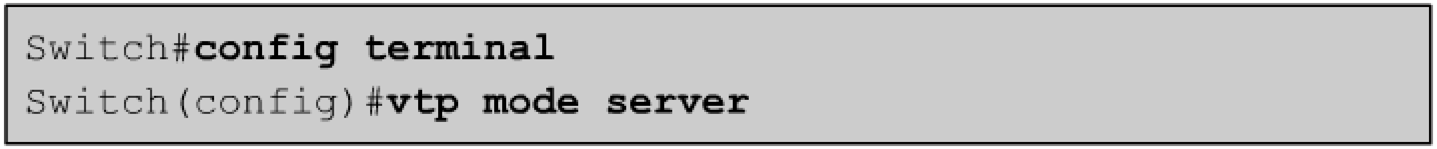
VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

- By default, management domains are set to a nonsecure mode, meaning that the switches interact without using a password.
- Adding a password automatically sets the management domain to secure mode.
- The same password must be configured on every switch in the management domain to use secure mode.

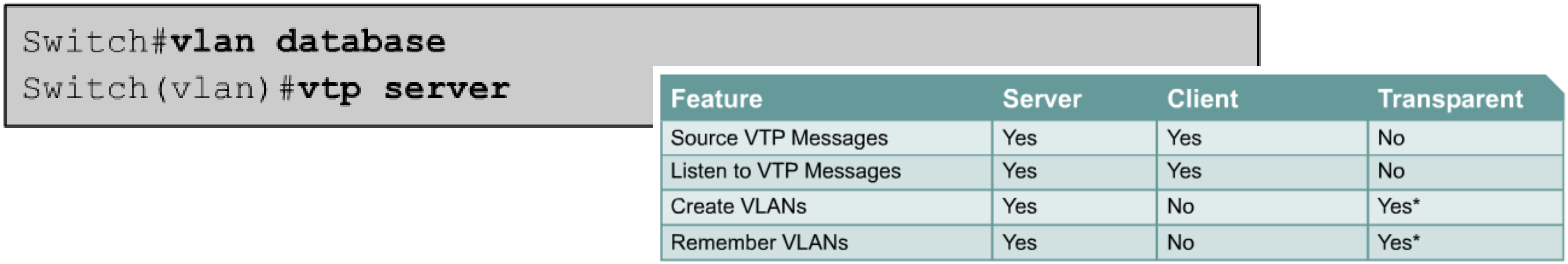
VTP configuration – VTP mode

VTP Configuration in global configuration mode:



```
Switch#config terminal
Switch(config)#vtp mode server
```

VTP Configuration in VLAN configuration mode:



```
Switch#vlan database
Switch(vlan)#vtp server
```

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

```
Switch#config terminal
Switch(config)#vtp mode [client|server|transparent]

Switch#vlan database
Switch(vlan)#vtp [client|server|transparent]
```

VTP Configuration - Overview

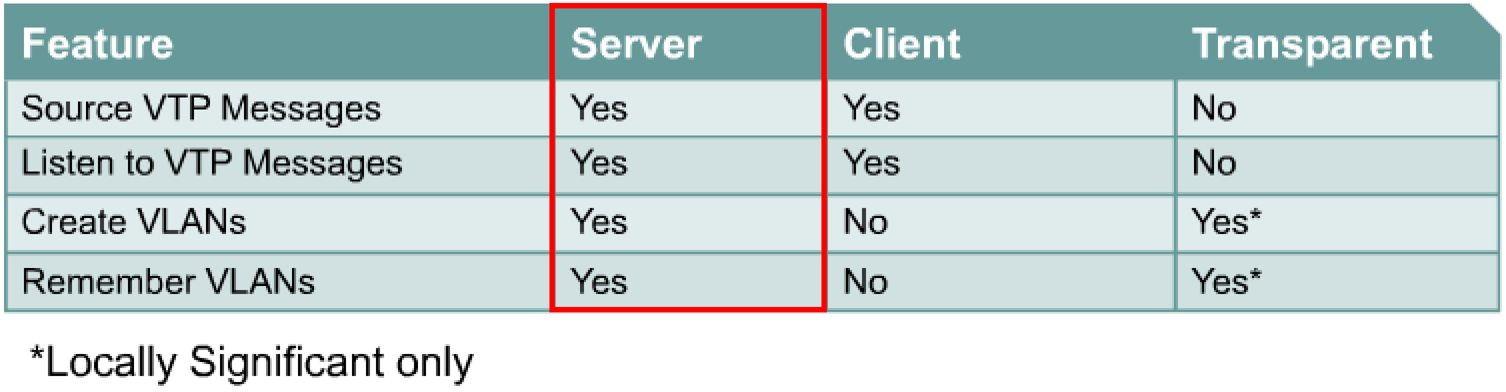
- VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```

- VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
Switch(vlan)#vtp server
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

VTP Operation

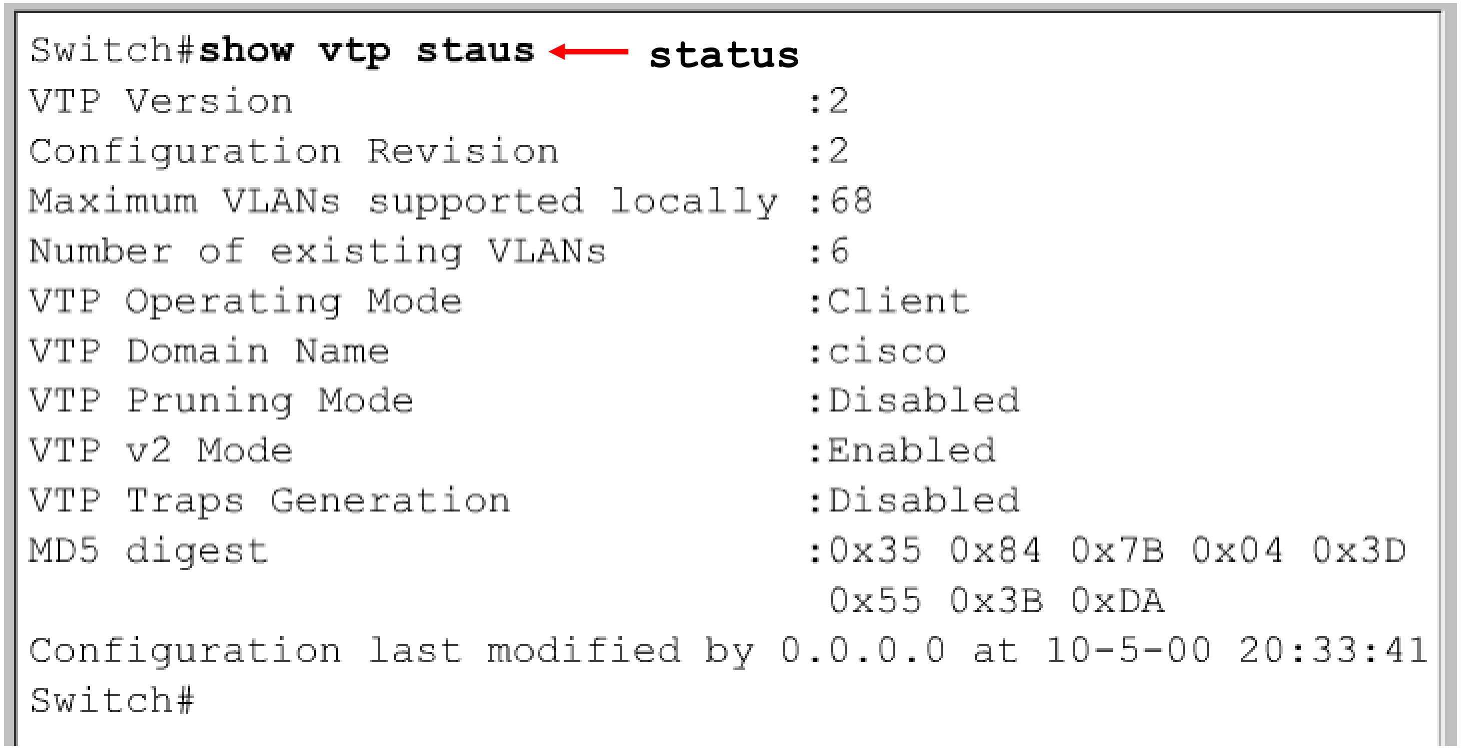


Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

- VTP switches operate in one of three modes:
  - Server
  - Client
  - Transparent
- **VTP servers** can create, modify, delete VLAN and VLAN configuration parameters for the entire domain.
- VTP servers save VLAN configuration information in the switch NVRAM. VTP servers send VTP messages out to all trunk ports.

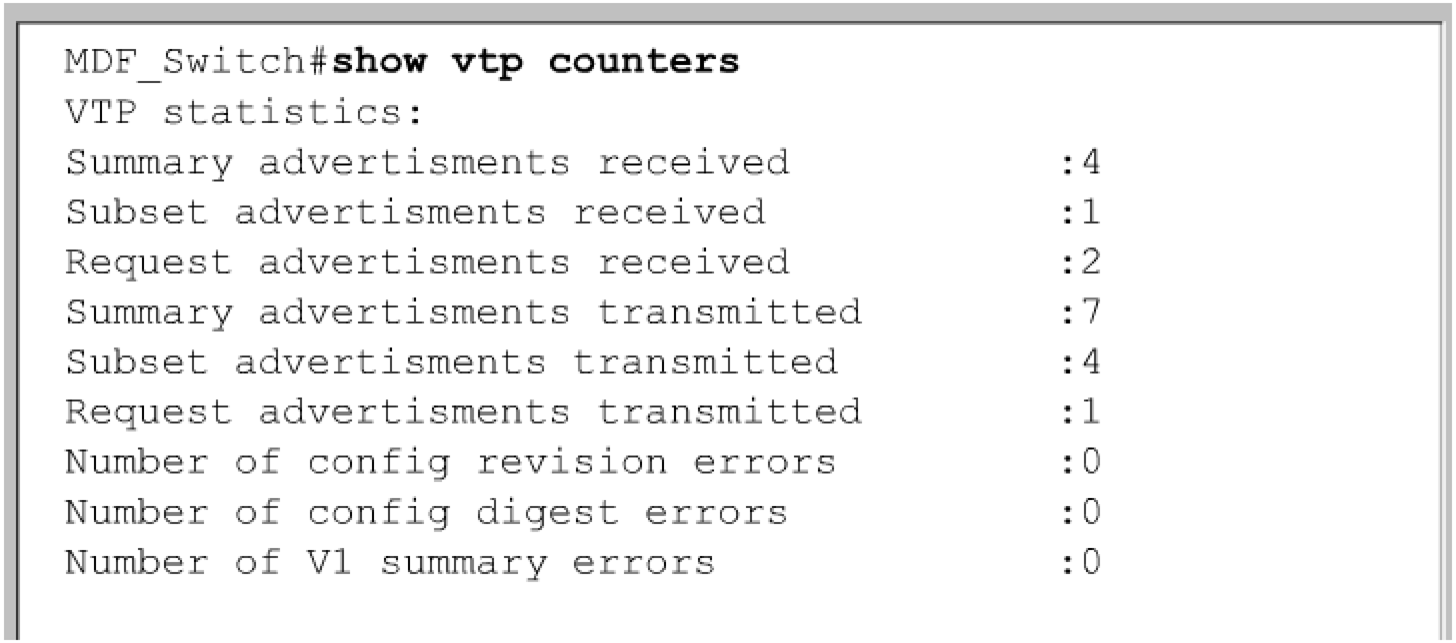
Verifying VTP



```
Switch#show vtp staus ← status
VTP Version                         :2
Configuration Revision              :2
Maximum VLANs supported locally     :68
Number of existing VLANs            :6
VTP Operating Mode                  :Client
VTP Domain Name                     :cisco
VTP Pruning Mode                    :Disabled
VTP v2 Mode                         :Enabled
VTP Traps Generation                :Disabled
MD5 digest                          :0x35 0x84 0x7B 0x04 0x3D
                                     0x55 0x3B 0xDA
Configuration last modified by 0.0.0.0 at 10-5-00 20:33:41
Switch#
```

- This command is used to verify VTP configuration settings on a Cisco IOS command-based switch.

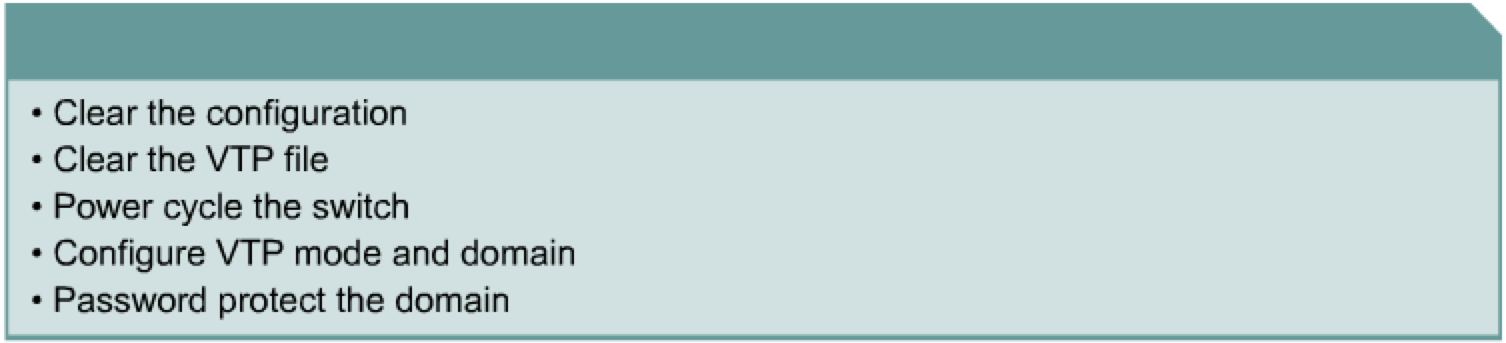
Verifying VTP



```
MDF_Switch#show vtp counters
VTP statistics:
Summary advertisments received          :4
Subset advertisments received           :1
Request advertisments received          :2
Summary advertisments transmitted       :7
Subset advertisments transmitted        :4
Request advertisments transmitted       :1
Number of config revision errors        :0
Number of config digest errors          :0
Number of V1 summary errors             :0
```

- This command is used to display statistics about advertisements sent and received on the switch.

Adding a switch to an existing VTP domain

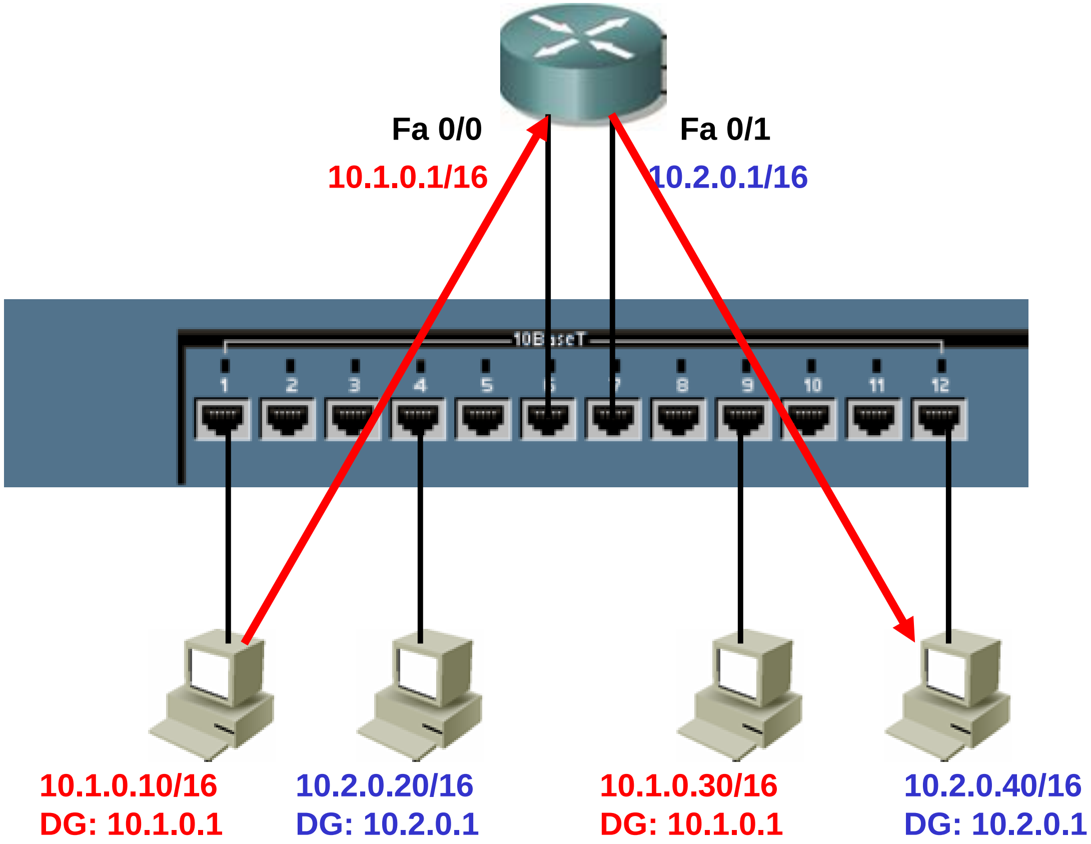


- Clear the configuration
- Clear the VTP file
- Power cycle the switch
- Configure VTP mode and domain
- Password protect the domain

- Use caution when inserting a new switch into an existing domain.
- In order to prepare a switch to enter an existing VTP domain, perform the following steps.
  - Delete the VLAN database
  - Erase the startup configuration
  - Power cycle the switch
- This will avoid potential problems resulting from residual VLAN configurations or adding a switch with a higher VTP configuration revision number that could result in the propagation of incorrect VLAN information.
- From the privileged mode, issue the **`delete vlan.dat`** and **`erase startup-config`** commands, then power cycle the switch.

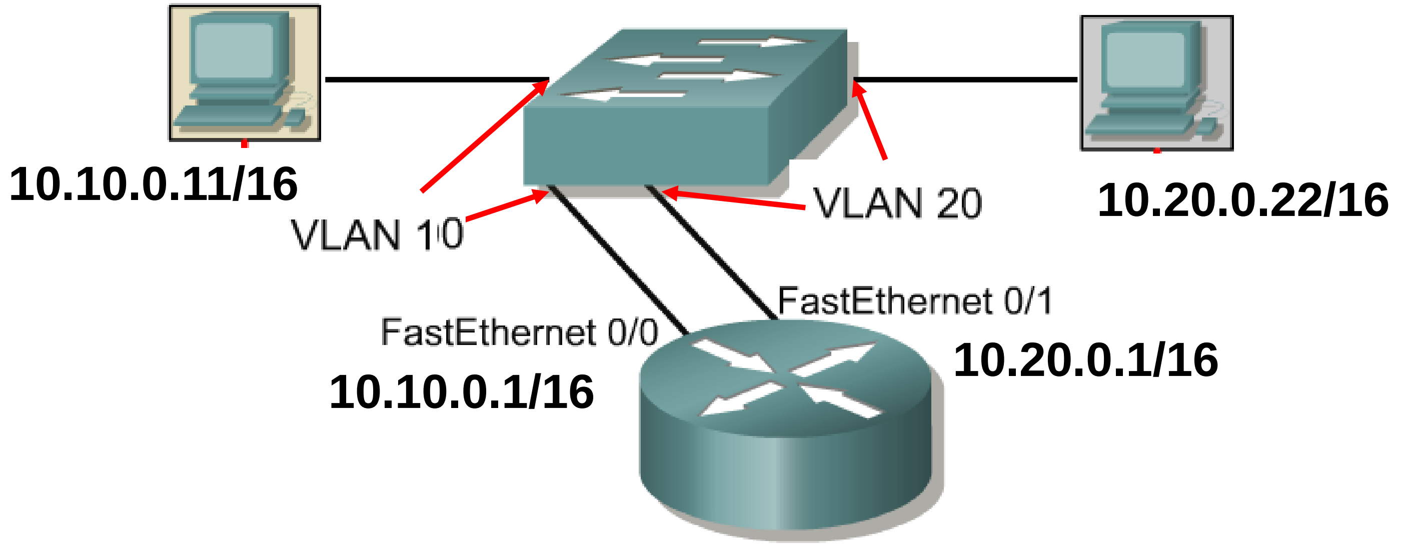
Inter-VLAN Routing

Inter-VLAN Routing



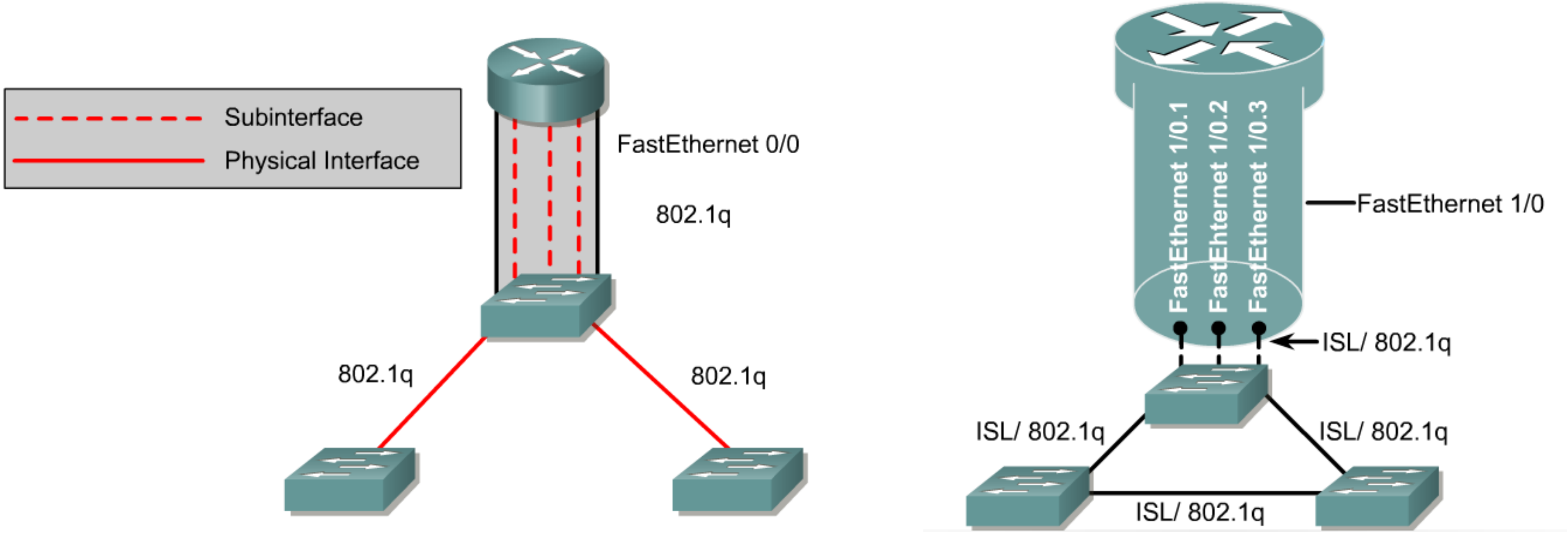
- When a node in one subnet or VLAN needs to communicate with a node in another subnet or VLAN, a router is necessary to route the traffic between VLANs.
- Without the routing device, inter-VLAN traffic would not be possible.

Inter-VLAN Routing - Non-trunk Links



- One option is to use a separate link to the router for each VLAN instead of trunk links.
- However, this does not scale well.
- Although it does load balance between VLANs, it may not make efficient use of links with little traffic.
- Be sure hosts and routers have the proper IP addresses, associated with the proper VLANs.
- It is common practice to assign VLAN numbers the same as IP addresses when possible.

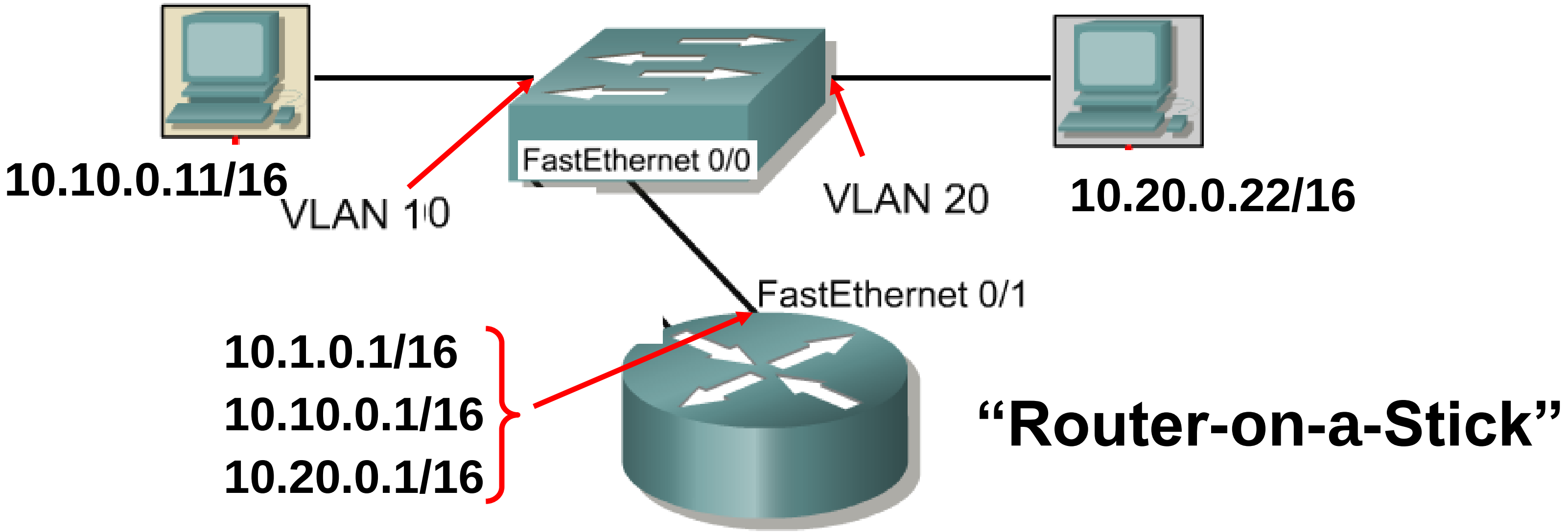
Physical and logical interfaces



- Subinterfaces on a router can be used to divide a single physical interface into multiple logical interfaces.
- Lower-end routers such as the 2500 and 1600 do not support subinterfaces.
- Each physical interface can have up to 65,535 logical interfaces.

```
Rtr(config)#interface fastethernet
  port/interface.subinterface
```

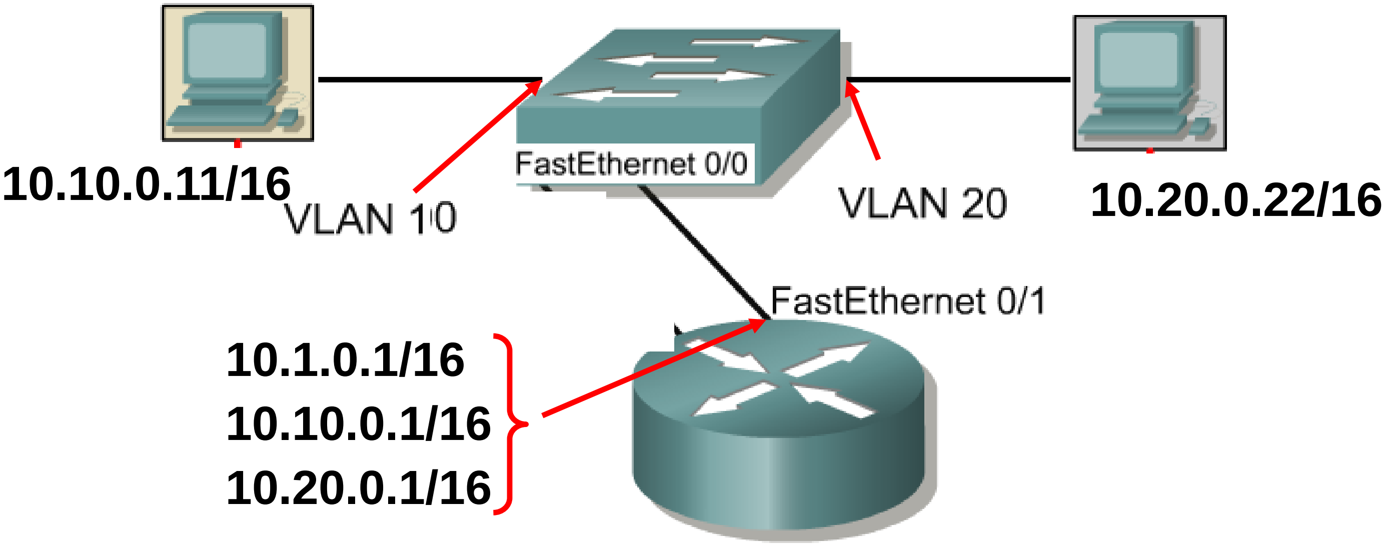
Inter-VLAN Routing - Trunk Links



```
Rtr(config)#interface fastethernet 0/1.1
Rtr(config-subif)#description VLAN 1
Rtr(config-subif)#encapsulation dot1q 1
Rtr(config-subif)#ip address 10.1.0.1 255.255.0.0
```

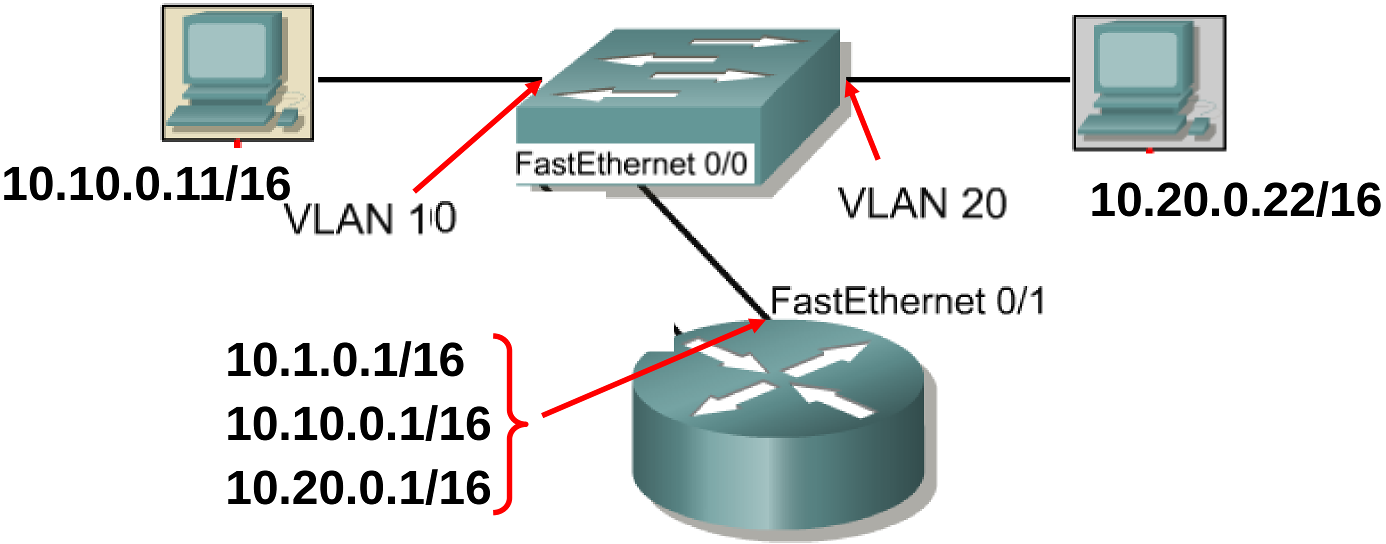
- It is recommended that the sub-interface value is the same as the VLAN.
- We will talk about VLAN 1 and the Management VLAN in a moment.
- It is recommended that VLAN 1 is not used for either Management traffic or user traffic.

Inter-VLAN Routing - Trunk Links



```
Rtr(config)#interface fastethernet 0/1.10
Rtr(config-subif)#description Management VLAN 10
Rtr(config-subif)#encapsulation dot1q 10
Rtr(config-subif)#ip address 10.10.0.1 255.255.0.0

Rtr(config)#interface fastethernet 0/1.20
Rtr(config-subif)#description Management VLAN 20
Rtr(config-subif)#encapsulation dot1q 20
Rtr(config-subif)#ip address 10.20.0.1 255.255.0.0
```

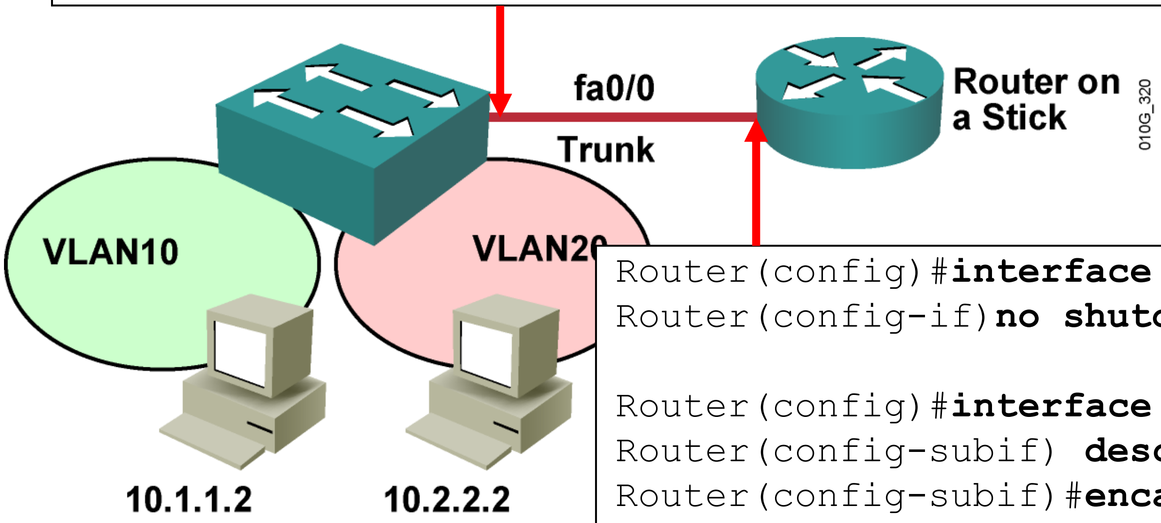
Inter-VLAN Routing - Trunk Links



```
switch(config)#interface FastEthernet 0/0
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
```

Router On A Stick: 802.1Q Trunk Link

```
switch(config)#interface FastEthernet 0/0
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
```

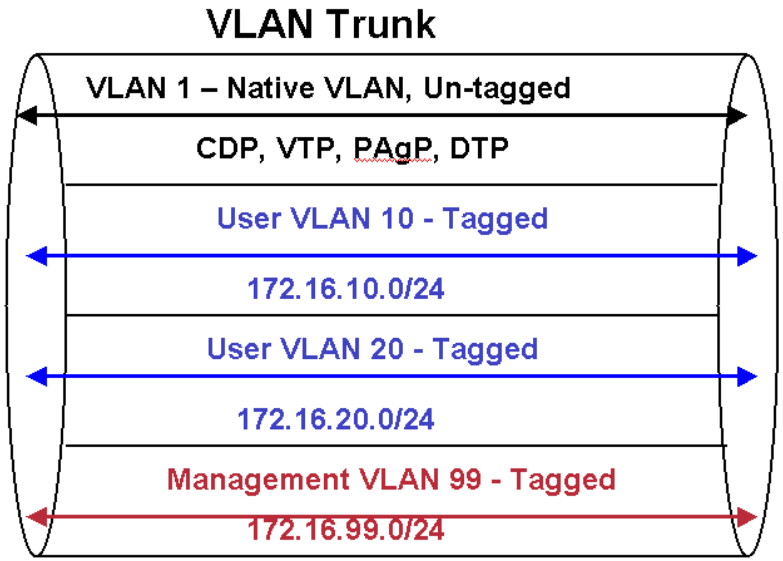


```
Router(config)#interface FastEthernet0/0
Router(config-if)no shutdown

Router(config)#interface FastEthernet 0/0.1
Router(config-subif) description VLAN 1
Router(config-subif)#encapsulation dot1Q 1 native
Router(config-subif)#ip address 10.10.1.1 255.255.255.0

Router(config)#interface FastEthernet 0/0.10
Router(config-subif) description VLAN 10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.10.10.1 255.255.255.0

Router(config)#interface FastEthernet 0/0.20
Router(config-subif)# description VLAN 20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.10.20.1 255.255.255.0
```

Addition VLAN Information

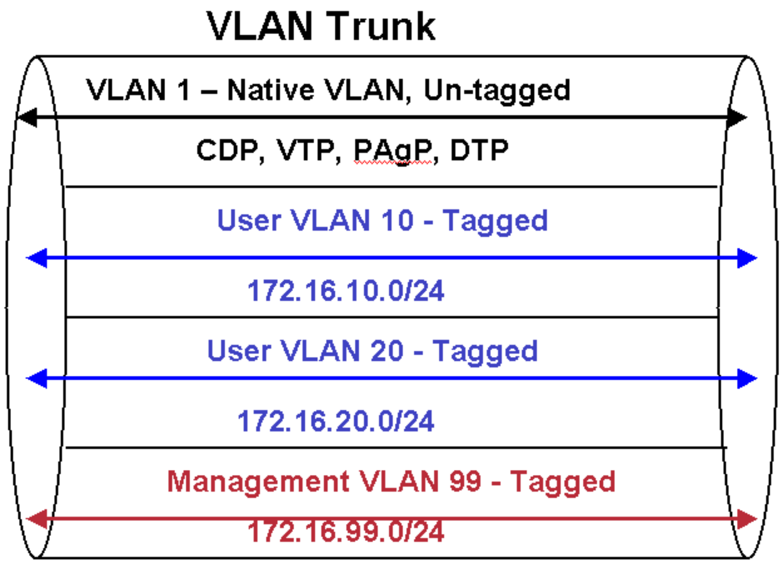
Cabrillo College

Management VLAN



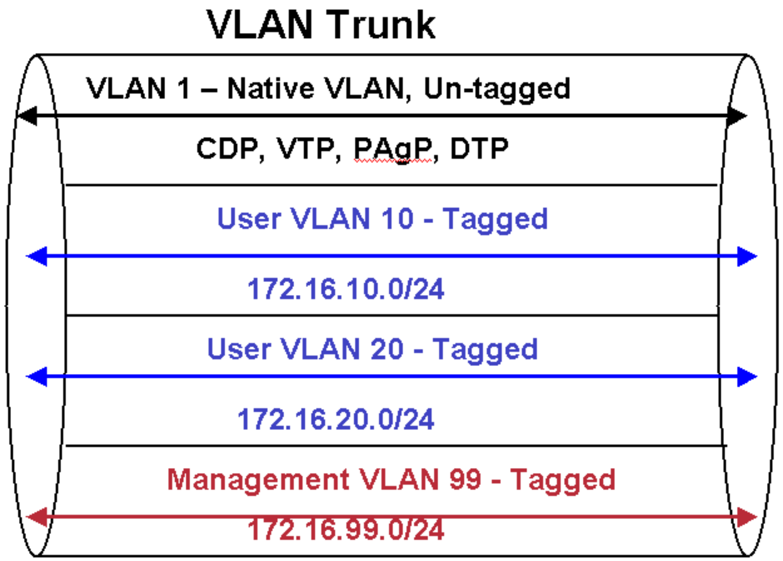
- For more information regarding VLAN 1, Management VLAN, default VLAN and the Native VLAN, see my article on my web site, **NativeVLAN.pdf**.
- This article will help explain the various types of VLANS and attempt to clear up some of this confusion.
- By default, all Ethernet interfaces on Cisco switches are on VLAN 1.
- On Catalyst switches all of these VLANs listed above default to VLAN 1, which can add to the difficulty of understanding their differences.

Management VLAN



- We won’t go into detail here but here are some guidelines.
- Notice that User VLANs have been configured for VLANs other than VLAN 1.
- The management VLAN refers to a separate VLAN for your switches and routers. This helps ensure access to these devices when another VLAN is experiencing problems.

Summary



- By default, VLAN 1 is the native VLAN and should only be used to carry control traffic, CDP, VTP, PAgP, and DTP. This information is transmitted across trunk links untagged.
- User VLANs should not include the native VLAN, VLAN 1. This information will be sent as tagged frames across VLAN trunks.
- The Management VLAN should be a VLAN separate from the user VLANs and should not be the native VLAN. This will insure access to networking devices in case of problems with the network.
- The subinterface on the router that is used to send and receive native VLAN traffic must be configured with the **`native`** option on the **`encapsulation`** interface command. This will let the router know that any frames coming in untagged belong to that subinterface and are a member of VLAN 1, the native VLAN. This is assuming that the native VLAN is the VLAN 1, the default native VLAN.

Trunking, VTP, DTP and Inter-VLAN Routing

Cabrillo College

CIS 83 (CCNP 3)

Fall 2006

Rick Graziani

Cabrillo College